KOTIKONEEN TIETOTURVA

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulun opinnäytetyö

Tietotekniikan koulutusohjelma

HAMK Riihimäki, kevät 2016

Jyri Lylykorpi

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

TIIVISTELMÄ

Riihimäki
Tietotekniikan koulutusohjelma
Tietoliikenneverkot

Tekijä Jyri Lylykorpi **Vuosi** 2016

Työn nimi Kotikoneen tietoturva

TIIVISTELMÄ

Suomalaisen yhteiskunnan palveluiden, tietojen ja työtehtävien siirtyminen verkkoon asettaa uusia vaatimuksia myös vankemmalle tietoturvan vaalimiselle. Tämän opinnäytetyön tarkoitus onkin toimia yleispätevänä oppaana modernin digiyhteiskunnan tietoturvavaatimuksista.

Työ on ensisijaisesti suunnattu henkilöille, jotka eivät luonnehtisi olevansa tietotekniikan ammattilaisia, mutta työ sisältää paljon lukemisen arvoisia huomioita myös tietotekniikkaan enemmän tutustuneille.

Opinnäytetyön tavoite on olla helposti luettava ja ymmärrettävä kokonaisuus, joka esittelee tietoturvaan liittyviä tärkeimpiä ilmiöitä, haasteita ja ratkaisuja.

Opinnäytetyössä esitetyt tiedot perustuvat kirjallisiin lähteisiin ja muutamiin verkkolähteisiin.

Avainsanat Tietoturva, kyberturvallisuus, tietosuoja

Sivut 43 s. + liitteet 0 s.

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Riihimäki
Degree Programme in Information Technology

ABSTRACT

Author Jyri Lylykorpi **Year** 2016

Subject of Bachelor's thesis Information security of the home computer

ABSTRACT

The need for even better information security has arisen because of changes in the Finnish society and the transition of services, data and work projects to the internet. The purpose of this thesis was to serve as a guide to the many information security challenges that the modern digital world offers.

This thesis is primarily targeted for people who would not consider themselves professionals in the field of information technology, but it also contains a lot of useful information for those who have more experience with computers.

The aim of this thesis was to showcase the most important aspects, challenges and possible improvements to one's information security in a manner that would be easy to understand.

This thesis is based on various literary sources as well as some web-based materials.

Keywords Information security, cyber security, data protection

Pages 43 p. + appendices 0 p.

SISÄLLYS

1 JOHDANTO

Modernin tietoyhteiskunnan kansalaistaito on asioida turvallisesti verkossa ja tunnistaa mahdollisia tietoturvaongelmia. Tietotekniikka on osa arkipäivästä elämää enemmän kuin koskaan aiemmin. Tämä helpottaa elämää, mutta tuo samalla myös useita uusia haasteita. Palveluiden, työtehtävien ja raha-asioiden siirryttyä verkkoon on tietoturvasta tullut asia joka koskettaa jokaista verkon käyttäjää. Tietoturvan ylläpito ei ole pelkästään tietokoneharrastelijoiden tehtävä, vaan nykypäivän yhteiskunnassa kaikilla on vastuu omien tietojen ja laitteiden turvaamisesta sekä turvallisesta verkossa asioimisesta.

Tämä työ pyrkii esittelemään lukijalleen tietoturvan merkityksen, esittelemään tietoturvan pyrkimykset sekä avaamaan tarkemmin syitä siihen, minkä vuoksi tietoturva koskettaa kaikkia. Opinnäytetyön tavoite on toimia oppaana turvalliseen asiointiin verkossa.

Työ on tarkoitettu sivistäväksi ja opastavaksi kokonaisuudeksi henkilöille, jotka eivät ole tietotekniikan ammattilaisia mutta joutuvat kuitenkin työskentelemään tietokoneilla työssä tai vapaa-ajalla. Työ voi toimia esimerkiksi opettavaisena tekstikokonaisuutena aloittelevalle netinkäyttäjälle verkon riskeistä tai tuoda uutta tietoa vähän tottuneemmallekin netin käyttäjälle esimerkiksi salasanakäytännöistä. Tämä opinnäytetyö pyrkii tuomaan helposti omaksuttavalla tavalla tavanomaisten – tietotekniikan alaan vähemmän perehtyneiden – henkilöiden tietoisuuteen modernin digiyhteiskunnan riskejä ja mahdollisesti tarjota yksinkertaisia keinoja torjua niitä.

Kokonaisuus jakautuu kuuteen eri osaan joiden tunteminen kuuluu tietoyhteiskunnan jäsenen yleissivistykseen. Ensimmäiseksi työssä selvennetään tietoturvan määritelmä ja merkitys. Tämän jälkeen pureudutaan tarkemmin vahvojen salasanojen muodostamiseen ja hallintaan, nettipalveluiden turvalliseen käyttöön ja tietoturvaa uhkaaviin tekijöihin kuten esimerkiksi haittaohjelmiin. Työ pitää myös sisällään käytännöllisiä vinkkejä joiden avulla tietokoneen turvallisuutta pystyy parantamaan. Lopuksi esitellään tärkeitä vinkkejä sosiaalisen median turvalliseen ja vastuulliseen käyttöön.

2 TIETOTURVA

Tietoturvasta on yhtäkkiä tullut keskeinen käsite tietokoneita ja ennen kaikkea internetissä sijaitsevia palveluita käytettäessä. Pankkiasioita, työasioita tai vaikkapa vapaa-ajalla sosiaalista mediaa käyttäessä törmää tietoturvan ja tietosuojan käsitteisiin. Usein kuitenkin jää vähän hämärän peittoon mitä nämä käsitteet edes todella tarkoittavat ja mistä tietoturvallisuudessa on kysymys.

2.1 Tietoturvallisuuden määritelmä

Tietoturvalla tarkoitetaan tietojen ja tietojärjestelmien suojausta. Tietoturva pyrkii järjestelmien ja palveluiden toimivuuteen ja turvalliseen käyttöön kaikenlaisissa olosuhteissa tietoturvan kolmen perustavoitteen mukaisesti. (Järvinen 2012, 12.) Nämä tavoitteet ovat tiedon luottamuksellisuus, tietojen eheys ja tiedon saatavuus, käytettävyys sekä toimivuus.

Luottamuksellisuudella tarkoitetaan tiedon pysymistä vain siihen oikeutettujen käyttäjien nähtävillä. (Järvinen 2012, 10.) Käytännössä tätä valvotaan esimerkiksi rajoittamalla käyttäjien pääsyä salasanoin, salauksin ja käyttäjiin kohdistuvin rajoituksin. Tietoturvan tavoitteena on pitää luottamukselliset tiedot, esimerkiksi potilas-, henkilö- sekä pankkitiedot vain asianomaisten tahojen käsiteltävinä eikä päästää arkaluontoisia tietoja vuotamaan vääriin käsiin.

Tiedon eheys on toinen tietoturvan tavoitteista. Eheään tietoon on kohdistunut vain oikeutettuja, oikeutettujen tahojen tekemiä mahdollisia muutoksia. Tietoturvan tavoitteena on estää ulkopuolisia tahoja tekemästä luvattomasti tietoihin muutoksia. (Järvinen 2012, 10.) Tavanomainen, varsin jokapäiväinen, esimerkki ehyen viestin rikkoontumisesta on sähköpostin mukana leviävät virukset. Toinen esimerkki eheysongelmasta on esimerkiksi kotisivujen tai sosiaalisen median profiilin sotkeminen ulkopuolisen tahon toimesta. Täten kotisivuihin tai profiiliin on kohdistunut muutoksia sellaisen tahon toimesta joka ei ole oikeutettu niitä tekemään. Sivun eheys on häpäisty.

Kolmas tietoturvan päätavoite on saatavuus, käytettävyys ja toimivuus (Järvinen 2012, 10). Nykyään kaikkien palveluiden ollessa ensisijaisesti verkossa on ehdottoman tärkeää varmistaa palveluiden toimivuus ja käytettävyys. Verkkopalveluiden toimimattomuus tulee yrityksille kalliiksi. Suurien yritysten palvelukatkoksista uutisoidaan näyttävästi, ja ne aiheuttavat yrityksille häpeää ja näiden käyttäjille harmaita hiuksia. Yritykset ajavat palveluitaan voimakkaasti verkkoon ja ihmiset tekevät mielellään ostoksensa, maksavat laskunsa ja lukevat uutisensa verkossa. Tämä asettaa jatkuvasti voimakkaamman paineen palveluiden saatavuudelle. Mitä enemmän käyttäjiä, sitä suurempi katastrofi mahdollinen käyttökatkos yritykselle on. Tavanomaisten laiterikkojen, yhteysongelmien ja sovelluksien kaatumisten lisäksi palvelun saatavuutta saattaa uhata myös ilkeämielisten ulkopuolisten tahojen toimet. Esimerkki tällaisesta toiminnasta on vaikkapa kohdistettu palvelunestohyökkäys, jossa kohde ikään kuin

hukutetaan kohdistamalla siihen huomattava määrä tarpeetonta liikennettä. Palvelu jumiutuu liiallisen kuorman alla ja rehelliset käyttäjät eivät pääse käsiksi palveluun. (Järvinen 2012, 179.)

Edellä mainittujen kolmen osatekijän lisäksi tietoturvan määritelmästä puhuttaessa mainitaan usein myös kaksi lisätekijää: kiistämättömyys ja pääsynvalvonta (Hakala 2006, 5).

Kiistämättömyydellä tavoitellaan tilannetta, jossa järjestelmän käyttäjä ei pysty kiistämään tekemäänsä tekoa (Hakala 2006, 5). Järjestelmien osalta pyritäänkin täten siihen, että tapahtumat voidaan myöhemmin todistaa tapahtuneeksi. Esimerkki tällaisesta on kyky nähdä, kuka on edellisen kerran muokannut tiedostoa.

Pääsynvalvonnalla rajoitetaan ulkopuolisten, kutsumattomien tahojen pääsyä käyttämään laitteita ja tietoliikenneyhteyksiä (Hakala 2006, 5). Varsinkin langattomien verkkojen yleistyminen on luonut pääsynvalvonnalle enemmän uusia haasteita. Tyypillinen pääsynvalvonnan haaste tavanomaisessa kotiverkossa on naapureiden verkon luvaton käyttäminen.

2.2 Tietoturvallisuuden merkitys

Tietoturvan merkitys voidaan nähdä kolmella tasolla. Nämä ovat henkilökohtainen tietoturva, työn tietoturva ja kansallisen tason tietoturva. Näillä tasoilla jokainen joutuu tekemisiin tietoturvan kanssa arkipäiväisessä elämässä. Henkilökohtaisen tason tietoturvan piiriin kuuluvat tavanomainen nettipalveluiden käyttö, tiedonhankinta, verkkoviestintä jne. Tietoturvan merkitys työssä on myös kasvanut. Lähestulkoon kaikissa ammateissa törmätään tietoturvaohjeisiin jotka koskevat salasanoja, yrityksen laitteiden ja yhteyksien käyttöä. Kansallinen taso lienee kaikista tärkein. Kansainvälisissä kriisitilanteissa saastuneet koneet ovat uhka koko maan turvallisuudelle, sillä maan ulkopuolelta tulevaa liikennettä on helpompi rajoittaa kuin maan sisäistä liikennettä. Mikäli kuitenkin koneet ovat jo aiemmin saastuneet, ne saattavat hyvinkin toimia ulkopuolisen vihollistahon kätyreinä maan rajojen sisällä. Tämä vaikeuttaa mahdollisen verkkohyökkäyksen torjuntaa merkittävästi. (Järvinen 2012, 13 – 15.) Tietoturva on täten yhteinen asia, johon kaikkien on syytä suhtautua asiallisella vakavuudella. Oman tietoturvan laiminlyönti ei aiheuta pelkästään ongelmia itse laiminlyöjälle, vaan saattaa aiheuttaa haasteita niin työpaikalla kuin myös kansallisella tasolla.

Tietoturvan vaatimukset kasvavat koko ajan. Markkinoille tulee jatkuvasti uusia laitteita ja palveluita, työpaikkojen tietojärjestelmät muuttuvat koko ajan haastavammaksi ja salasanojen määrä kasvaa mahdottomaksi muistaa. Palvelut siirtyvät joukolla verkkoon. Miltei kaikki palvelut löytyvät verkosta: ostokset, raha-asiat, verkostoituminen ja vapaa-ajan harrastukset ovat kaikki mitä suurimmassa määrin siirtyneet verkkoon. Tämä kaikki asettaa käyttäjille lukuisia uusia vaatimuksia jotta verkossa asioiminen sujuisi luontevasti ja turvallisesti.

Tietoturva-asioista uutisoidaan usein lehdistössä maalaillen kuvia suurista hyökkäyksistä merkittävien yritysten palveluihin tai suuren mittaluokan haavoittuvuuksista yleisesti käytetyissä ohjelmissa. Todellisuudessa kuitenkin merkittävin tietoturvaongelma on tavanomaisten käyttäjien tekemät inhimilliset virheet. Kiireessä helposti oikaistaan mutkia tietoturvan kustannuksella, eikä esimerkiksi tarkisteta sosiaaliseen mediaan kirjoitetun viestin sisältöä huolella. Näin arkaluontoistakin materiaalia saattaa joutua kaikkien katseltavaksi. Tietokoneen näytölle pomppaa yllättäen viesti, jonka sisältöä käyttäjä ei oikein ymmärrä ja puolihuolimattomasti kuittaa viestin sisällön painamalla kyllä. Yrityksen uudet tietojärjestelmät ovat hankalasti ymmärrettäviä, sillä kiireessä koulutus ja niihin perehtyminen kunnolla on saattanut jäädä tekemättä. Nämä kaikki ovat varsin tavanomaisia tietoturvan puutteita ja ongelmia, joihin tavanomainen käyttäjä törmää päivittäisessä elämässä.

Tietoturva kalskahtaa usein tekniseltä asialta, jonka hoitaminen kuuluu insinööreille eikä suinkaan tavalliselle käyttäjälle. Todellisuudessa käyttäjä itse on päävastuussa tietoturvansa tasosta. Mikään määrä tietoturvaa kohentavia ohjelmia, estoja ja laitteita ei pysty pelastamaan käyttäjää itseltään mikäli tämä toimii jatkuvasti terveen järjen ja suositeltujen käytäntöjen vastaisesti. Suurin vastuu turvallisesta toiminnasta on käyttäjällä.

3 SALASANAT

Modernin tietoyhteiskunnan jäsenelle salasanat ovat arkipäiväinen tunnistautumisen väline. Muistettava on niin henkilökohtaisten palveluiden salasanat kuin myös tärkeät työhön liittyvät tunnukset. Salasana on ikään kuin nykypäivän avain useimpiin työn ja vapaa-ajan tärkeisiin resursseihin. Täten salasanat muodostavat yhden tärkeimmistä tietoturvan osa-alueista. Salasanojen luomiseen insinöörit yrittävät antaa ohjeita ja vaatimuksia, mutta lopulta vastuu turvallisen salasanan luomisesta on käyttäjällä itsellään.

Salasanojen käyttöön liittyy kuitenkin lukuisia ongelmia. Yksi näistä on se, että salasana ei ole järin varma keino varmistaa käyttäjän olevan se joka hän väittää olevansa. Kirjautuminen ainoastaan varmistaa sen, että henkilö ruudun toisella puolella tietää tunnistautumiseen käytetyn oikean sanan. Täten salasana jättää keinona varmentaa käyttäjä oikeaksi paljon toivomisen varaa. Kirjautumiseen käytetyt tiedot, kuten sähköpostitili tai käyttäjätunnus ovat yleensä yleistä tietoa ja ainoastaan salasana erottaa oikean käyttäjän mahdollisesta tunkeilijasta. Tämä tekee vahvan salasanan luomisesta erityisen tärkeää.

Merkittävä salasanoihin liittyvä ongelma lienee käyttäjien taipumus unohdella salasanojaan. Tämä on varsin inhimillinen ongelma, sillä mikäli noudattaa tietoturvahenkilöiden antamaa nyrkkisääntöä jonka mukaan jokaiseen palveluun tulisi luoda uusi salasana, kasaantuu muistettavien salasanojen määrä jossain vaiheessa sietämättömäksi. Pitkän kesäloman jälkeen työntekijä on saattanut unohtaa kaikki tärkeät työhön liittyneet salasanat. Täten tunnistautuminen epäonnistuu, vaikka tietoihin tai palveluun pyrkii käsiksi henkilö jonka pitäisi olla niihin oikeutettu.

Toinen salasanoihin liittyvä huolenaihe on se, että ihmisillä on vasten tervettä järkeä taipumus luovuttaa salasanojaan muiden ihmisten tietoisuuteen. Salasanan tarkoitus on toimia yksilöllisenä todentamisen välineenä. Ystävälle tai työtoverille oman salasanan luovuttaminen tuntuu tietenkin harmittomalta. Se on kuitenkin lähtökohtaisesti huono idea, varsinkin jos käyttää samaa salasanaa useissa eri palveluissa. Mikä estäisi ystävää kokeilemasta samaa salasanaa esimerkiksi sosiaalisen median palveluiden urkkimiseen?

Kolmas ongelma on, että useimmiten salasanan vuotaminen väärinkäyttäjän käsiin ei paljastu heti. Tavanomaisen avaimen tai kulkukortin hukkaamisen huomaa heti ja henkilö voi ryhtyä asianmukaisiin toimiin tilanteen korjaamiseksi. Salasana voi sisäänpääsyn keinona olla sekä väärinkäyttäjän kuin myös tilin varsinaisen omistajan käytössä. Väärinkäyttäjä saattaa lukea yksityisiä tietoja, sähköposteja ja keskusteluja tilin varsinaisen käyttäjän huomaamatta mitään. Mahdollista on myös, että tunkeilija vaihtaa salasanan estäen samalla alkuperäisen käyttäjän pääsyn.

3.1 Hyvät salasanakäytännöt

Paljon puhutaan vahvoista salasanoista ja annetaan käyttäjille mitä erilaisimpia kriteerejä, jotta he muodostaisivat riittävän vaikeasti murrettavia tai arvattavia salasanoja. Tavanomaisesti salasanojen osalta on käytetty seuraavia vaatimuksia:

1. Salasanan tulisi olla riittävän pitkä ja käyttää erikoismerkkejä
2. Salasanojen säännöllinen vaihtaminen
3. Salasanojen kirjoittaminen muistiin esim. paperille on kiellettyä
4. Joka palvelussa tulisi käyttää omaa salasanaa (Järvinen 2012, 114.)

Käytäntö on kuitenkin osoittanut, että nämä vaatimukset ovat kohtuuttoman tiukkoja ja käyttäjät todennäköisesti ajautuvat rikkomaan niitä. Tavanomaisesti tietoturvaa pyritään kohentamaan lisäämällä salasanan vaihtovälejä ja pidentämällä salasanojen minimipituutta. Käyttäjät tuppaavat ahdistumaan, kun toistuvasti pitää yrittää keksiä uusia ja pidempiä salasanoja. Tiukkojen salasanakriteerien ja turhauttavan tiheiden vaihtovälien sijaan maalaisjärjen käyttö ja käyttäjien tiedon lisääminen johtanee toimivimpaan ratkaisuun.

Mitkä seikat sitten ovat olennaisia hyvän salasanan luomisessa? Salasanan pituus on yksi merkittävimmistä seikoista turvallista salasanaa kehiteltäessä. Tämä juontaa juurensa pyrkimyksestä torjua ns. brute force -hyökkäyksiä, jossa hakkeri pyrkii tietokoneen avulla kokeilemaan kaikkia mahdollisia merkkiyhdistelmiä kunnes oikea salasana löytyy. Mitä pidempi salasana on, sitä enemmän on läpikäytäviä vaihtoehtoja. Täten mitä pidempi salasana, sitä kauemmin sen selvittämiseen kuluu aikaa. (Järvinen 2012, 114.)

Hyvä käytäntö salasanaa luotaessa on lisätä salasanaan numeroita kirjainten lisäksi. Tällä on oleellinen vaikutus salasanan turvallisuuteen, sillä täten brute force -hyökkääjä joutuu käymään läpi myös numerot löytääkseen oikean salasanan. (Järvinen 2012, 114.) Yleisesti käytetty hyväksi todettu tapa on esimerkiksi korvata kirjaimet numeroilla. Esimerkiksi salasana ”tietoturva” muuttuu vahvemmaksi salasanaksi kirjoittamalla tämä numeroita ja isoja kirjaimia hyväksi käyttäen ”T13t0Turv4”. Hyvä tapa tehdä salasanasta vielä vaikeammin murrettava ja turvallisempi on ottaa käyttöön näppäimistön erikoismerkit (Järvinen 2012, 114). Näihin voidaan lukea kaikki näppäimistön merkit jotka eivät ole kirjaimia tai numeroita.

Eräs vaihtoehto on käyttää salasanana kokonaista lausetta, sillä salasanan ei tarvitse olla yksittäinen sana (Järvinen 2012, 114). Tässä tapauksessa salasana olisi esimerkiksi ”Tällä sanalla pääsen sisään sähköpostiini”. Tällainen salasana on helppo muistaa ja kirjoittaa. Samalla tämä on myös hankala murtaa tai vaikkapa selvittää olan yli kurkkimalla. Toinen vaihtoehto on muodostaa salasana pitkän lauseen sanojen alkukirjaimista (Järvinen 2012, 120). Esimerkiksi lause ”Syntymäpäiväni on 10. lokakuuta 1980” muodostuu täten vahvaksi salasanaksi ”SyOn10lo-80!”.

Salasanojen suhteen ohjenuorana on usein esitetty, että jokaiseen palveluun tulisi valita uniikki salasana (Järvinen 2012, 118). Täten, mikäli katastrofi tapahtuu ja yhden palvelun salasana vuotaa ulkopuolisen tahon käsiin, ei kaikkien muiden tilien turvallisuus ole uhattuna. Tämä rajoittaa mahdollisen vahingon määrää huomattavasti. Todellisuudessa ihmiset käyttävät lukuisia palveluita ja lienee absurdia kuvitella, että he keksisivät joka palveluun yksilöllisen salasanan ja vielä muistaisivat sen. Realistisempi ohje salasanojen suhteen on kategorisoida palvelut siten, että luo uniikin salasanan erittäin tärkeisiin palveluihin (työ, sähköposti, raha-asioita sisältävät palvelut jne.) ja vähemmän tärkeissä palveluissa (keskustelupalstat, nettilehdet jne.) käyttää samaa salasanaa jos se helpottaa muistamista.

Vanha kiveen hakattu sääntö on, että salasanat tulisi muistaa ulkoa eikä niitä missään nimessä tulisi kirjoittaa ylös mihinkään. Todellisuudessa tietoturvan kannalta suurempi riski on unohtunut salasana, eikä suinkaan mahdollinen salasanamuistilappu lipaston laatikossa. Tietoturvan kannalta parempi on käyttää hyviä, vaikeammin muistettavia salasanoja ja kirjoittaa ne muistiin paperille kuin käyttää kaikissa palveluissa luokattoman huonoja salasanoja. (Järvinen 2012, 117.) Hyvä käytäntö tietenkin olisi, että tällaisessa muistilapussa olevat salasanat eivät olisi suoraan yhdistettävissä palveluihin joissa niitä käytetään.

Varsinkin tärkeitä salasanoja tulisi vaihtaa säännöllisesti, vaikkapa 3 kuukauden välein. Mikäli salasana on vuotanut käyttäjän huomaamatta väärinkäyttäjälle, salasanan vaihtaminen estää väärinkäytön jatkumisen. Samalla perusteella käyttäjälle usein esitetään salasanan vaihdon yhteydessä järjestelmän toimesta vaatimus, että uusi salasana ei voi olla sama kuin jokin edellisistä salasanoista. (Rousku 2014, 179.) Säännöllinen salasanan vaihtaminen edellyttää tietenkin käyttäjältä vähän ylimääräistä vaivannäköä, mutta on kuitenkin suositeltu varatoimenpide varsinkin tärkeiden palveluiden suojelemiseksi.

3.2 Huonot salasanakäytännöt

Valitettava tosiasia on, että useilla käyttäjillä on lukuisia huonoja tapoja salasanojen suhteen. Tavanomaisesti käyttäjä yrittää päästä helpommalla salasanaa keksiessään ja kuvitellen yksinkertaisen salasanan olevan merkittävästi helpompi muistaa kuin turvallisen pitkän salasanan. Todellisuudessa esimerkiksi pitkän lauseen alkukirjaimista muodostettu turvallinen salasana on aivan yhtä helppo muistaa. Järjellisen sanakirjasta löytyvän sanan käyttäminen salasanana on yleisesti ottaen erittäin huono idea, sillä hakkerit useimmiten tunkeutumista yrittäessään käyvät läpi sanalistoja (Rousku 2014, 180).

Muita tyypillisiä, mutta todella huonoja taipumuksia salasanojen suhteen ovat esimerkiksi oman nimimerkin tai palvelun nimen käyttäminen salasanana. (Järvinen 2012, 118.) Käyttäjästä voi tuntua helpolta valita salasanaksi esimerkiksi juuri oma nimimerkki, sillä sehän on luonnollisesti helppo sana muistettavaksi. Todellisuudessa nimimerkki, on se sitten kirjoitettu etu- tai takaperin, on niin yleinen salasana että mahdollinen tunkeilija todennäköisesti yrittää kirjautua sillä sisään ensimmäisten yritysten joukossa.

Huonoista salasanoista puhuttaessa lienee myös aiheellista huomauttaa, että yleisesti tiedettyjen henkilökohtaisten tietojen käyttäminen salasanana on todella huono idea. Täten esimerkiksi sähköpostiosoitteen, oman syntymävuoden, etunimen tai auton rekisterinumeron käyttäminen salasanana on riskialtista puuhaa. Näistä tekee riskialttiin salasanana se, että nämä tiedot ovat joko jo kaikkien tuttujen tiedossa muutenkin tai selvitettävissä nopeasti esimerkiksi sosiaalisen median profiilista. (Järvinen 2012, 119.) Salasanan unohtumisen varalta palvelut usein pyytävät käyttäjää antamaan vastauksen käyttäjän valitsemaan turvakysymykseen. Tämä kysymys sitten esitetään käyttäjälle, mikäli tämä joutuu käyttämään salasanan palautustoimintoa. Ongelma näiden kysymysten osalta on siinä, että käyttäjien vastaukset ovat usein helposti arvattavissa tai löydettävissä esimerkiksi sosiaalisesta mediasta. Potentiaalisen uhrin suosikkiurheilija tai koiran nimi on usein kaiken kansan nähtävillä sosiaalisessa mediassa. (Järvinen 2012, 129.) Turvakysymyksen toimivuuden kannalta ei ole olennaista onko syötetty vastaus totta. Tietoturvan näkövinkkelistä paras tapa olisi käyttää turvakysymyksessä vastausta jonka vain itse tietää. Mitä kauempana todellisuudesta vastaus on, sitä hankalampi se on tunkeilijan arvata.

Tietoturvavalistuksesta, koulutuksesta ja ohjeista huolimatta kaikkien aikojen kestosuosikki salasanojen listalla Suomessa on kuitenkin 123456. Toisena yleisimpien salasanojen listalla on salasana ja kolmantena qwerty. (Rousku 2014, 75.) Näiden jälkeen yleisimpien listalle kiilaavat seuraavaksi useimmiten eräät voimasanat ja käyttäjien etunimet. Toisin sanoen: näitä erittäin huonoja salasanoja kannattaa välttää.

4 NETTIPALVELUIDEN TURVALLINEN KÄYTTÖ

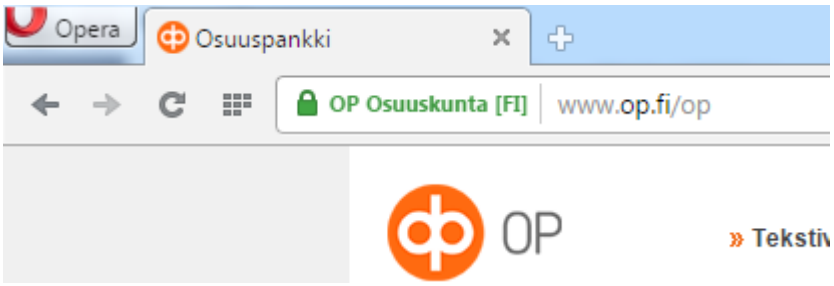
Tärkeiden ja tietojen luottamuksellista käsittelyä vaativien palveluiden siirtyminen verkkoon on asettanut entistä suuremmat vaatimukset nettiasioinnin turvaamiselle. Karua todellisuutta kun on, että pankki- ja raha-asioiden siirtyminen verkkoon on suunnannut myös rikollisten tahojen mielenkiinnon verkkorikollisuuteen. Näiden rikollisten erikoisalaa useimmiten ovat käyttäjien pankki- ja muut henkilökohtaiset tiedot. Tämä asettaa verkossa asioinnille tarkkoja vaatimuksia, sillä käyttäjien henkilökohtaisten tietojen päätyminen rikollisten käsiin olisi katastrofi.

Verkkosivujen ja selainten turvallisuutta on pyritty parantamaan salauksilla, varmenteilla ja suojaohjelmilla. Näiden kaikkien ominaisuuksien tarkoitus on parantaa verkossa asioinnin turvallisuutta. Yksi turvallisen netissä asioinnin perusedellytyksistä on, että sivulliset henkilöt eivät pääse urkkimaan verkossa tapahtuvan toiminnan sisältöä. Näin esimerkiksi tärkeät pankkitilin tiedot tai salasanat liikkuvat salatussa muodossa palvelun ja käyttäjän koneen välillä. Tärkeää on myös varmistua käytettyjen sivujen oikeellisuudesta ja turvallisuudesta. Täten käyttäjä voi tietää käyttävänsä oikeaa palvelua, eikä epähuomiossa syötä tietojaan valesivulle. Tärkeä osa turvallisen nettiasioinnin mahdollistamista on käyttäjän suojelu haitallisiksi tiedetyiltä verkkosivustoilta. Käytännössä selain siis pyrkii estämään käyttäjän pääsyn vaarallisille sivuille joiden tiedetään sisältävän turvallisuutta uhkaavia elementtejä, esimerkiksi haittaohjelmia.

4.1 SSL

SSL on lyhenne sanoista Secure Sockets Layer. Kyseessä on salausprotokolla, joka salakirjoittaa nettiselaimen ja www-palvelimen välillä tapahtuvan liikenteen. SSL käyttää tavanomaisesti 128-bittistä avainta salaukseen ja on täten murtovarma tapa salata liikennettä. (Järvinen 2006, 67.) SSL:n suojatessa liikennettä ulkopuoliset tahot eivät näe mitä esimerkiksi pankkipalvelun ja kotitietokoneen välillä tapahtuu. Täten rahansiirrot ja ostokset voidaan tehdä yksityisesti ja turvallisesti.

Hyvänä nyrkkisääntönä voisi pitää sitä, että SSL-salauksen tulisi turvata asiointia aina kun liikutellaan yksityisiä tietoja netissä. Varsinkin pankkiasioita hoidettaessa tulisi aina varmistaa salauksen kytkeytyminen päälle. Salauksen käyttöönotto tapahtuu aina palvelimen aloitteesta, eikä käyttäjällä tavanomaisesti ole siihen vaikutusta (Järvinen 2006, 68). Täten SSL-salauksen puuttuminen sivustolta jolla se tavanomaisesti on käytössä (esim. pankki), on usein merkki tietoturvaongelmasta. Käyttäjä voi itse todentaa salauksen olevan käytössä kiinnittämällä huomionsa muutamaan seikkaan. Helpoiten salauksen huomaa siitä, että osoiteriville ilmestyy lukon kuva (kuva 1). Myös osoiterivillä sivuston osoite alkaa kirjaimilla HTTPS, mikä kertoo käyttäjälle että käytössä on salattu HTTPS-protokolla ja täten SSL-salaus.

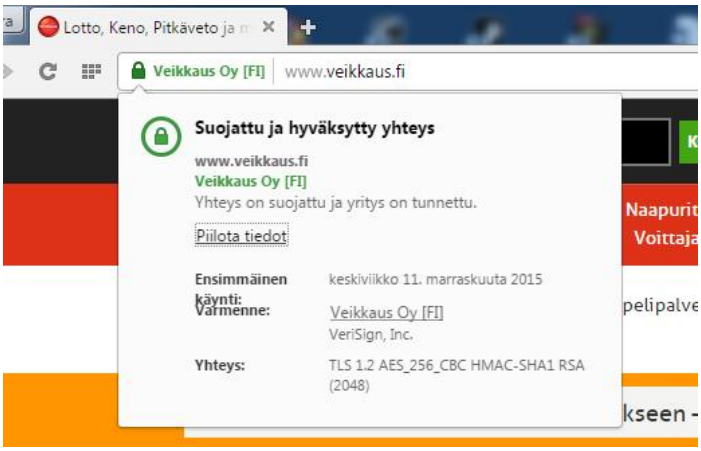


Kuva 1. Vihreästä lukon kuvasta on pääteltävissä SSL-salauksen olevan käytössä. Lukon puuttuminen esim. pankin palveluita käytettäessä voi olla merkki tietoturvaongelmasta.

4.2 Varmenteet

Luottamuksellisia tietoja liikuteltaessa verkon yli on tärkeää varmistua myös siitä, että käytettävä palvelu itsessään on todellisuudessa juuri se palvelu joka väittää olevansa. Täten käyttäjillä on kyky varmistua siitä, että käyttäessään esimerkiksi valitsemansa pankin verkkopalvelua he asioivat juuri kyseisen pankin palvelussa eivätkä esimerkiksi jonkinlaisessa valepalvelussa. Tämä on myös olennainen osa SSL-tekniikkaa. Varmenteita käyttämällä varmistutaan palvelun oikeellisuudesta. Varmenteita myöntävät viralliset tahot, jotka ovat tarkistaneet palvelun ja myöntäneet tälle todistuksen oikeellisuudesta. Tämä todistus oikeellisuudesta, varmenne, sijoitetaan palvelimelle josta käyttäjän selain pyytää varmennetta käyttäjän pyrkiessä sivulle. Palvelin toimittaa selaimelle varmenteen, josta selain voi todeta sivuston oikeellisuuden. (Järvinen 2012, 59.)

Varmenteesta voidaan todeta tarkalleen, minkä yrityksen hallinnoimasta palvelusta on kyse ja kuka on todentanut palvelun oikeellisuuden (kuva 2).



Kuva 2. Sivuston varmenne on kunnossa ja yritys on tunnettu. Varmenteen on allekirjoittanut Verisign-niminen yritys.

Kaikenlaisiin varmenteisiin liittyviin ilmoituksiin olisi syytä suhtautua vakavasti, sillä kyseessä on olennainen osa SSL-suojausta ja verkossa asioinnin turvaamista. Varmenteen ja suojauksen puuttuminen esim. pankin sivuilta on huolestumisen paikka. Tavanomaisimpia varmenteisiin liittyviä virheilmoituksia ovat seuraavat:

1. Varmenne on vanhentunut
2. Varmenteen osoite ei vastaa www-sivun osoitetta
3. Varmenteen myöntäjä on taho, johon selain ei luota (Järvinen 2012, 62.)

Ensimmäinen virheilmoitus johtuu usein sivuston ylläpidon huolimattomuudesta, sillä sivuston varmenne on päässyt vanhentumaan kun ylläpito ei ole muistanut uusia varmennetta ajoissa. Varmenteet ovat tavanomaisesti voimassa kerrallaan vuoden tai kaksi (Järvinen 2012, 62). Näin voi käydä hyvin luotettavienkin toimijoiden sivulla, mikä tietysti on jonkinlainen häpeän aihe kyseisen palvelun ylläpidolle.

Mikäli varmenteen osoite ei vastaa itse sivuston osoitetta, kyseessä saattaa olla huijaus. Toisinaan kyse voi olla ylläpidon tekemästä inhimillisestä virheestä, jossa www-palvelimen nimi on muuttunut varmenteen oston jälkeen.

Mikäli selain ei luota varmenteen myöntäjään sivun käyttöön kannattaa suhtautua varauksella. Selaimet tunnistavat luotettavan varmenteen myöntäjän listasta, joka jokaiseen selaimeen on rakennettu sisään (Järvinen 2012, 63). Selain tarkistaa tiedoistaan, mitä varmenteiden myöntäjiä se pitää luotettavina. Mikäli listalta ei löydy kyseisen sivuston varmenteen myöntäjää, pitää selain tätä epäluotettavana. Palvelut voivat myöntää myös varmenteen itse itselleen, mahdollistaen täten tietojen suojauksen. Tällainen varmenne ei kuitenkaan ole virallisen tahon myöntämä ja siksi lähtökohtaisesti epäluotettava. Ilman ulkopuolisen tahon kontrollia palvelu voi ilmoittaa olevansa itse ihan mitä tahansa. Käytännössä kuitenkin tällaiset itse myönnetyn varmenteen sivustot voivat olla myös luotettavia ja virallinen varmenne on jätetty hakematta esim. säästösyistä. Perustavaa laatua olevana sääntönä voidaan pitää, että turvallisten ja virallisten tahojen palvelut käyttävät aina virallista varmennetta. Mikäli varmenteen tai salauksen kanssa ilmenee ongelmia, on syytä pysähtyä ja tutkia tilannetta tarkemmin.

4.3 Selaimen tietoturva

Kuten jo aiemmin on tullut ilmi (luku 4), verkkoselaimen osuus tietokoneen tietoturvan ylläpitämisessä on huomattava. Kaikkiin uusimpiin selaimiin on rakennettu ominaisuuksia, jotka pyrkivät suojaamaan käyttäjää verkon vaaroilta. Jotta selain voisi tehdä tämän osuuden työstään oikein, tulee käyttäjän kuitenkin huolehtia selaimen päivittämisestä ajankohtaisimpaan versioon.

Useimmissa selaimissa on sisäänrakennettu tietoturvaominaisuus, joka estää käyttäjän pääsyn tunnetuille vaarallisille sivuille. Selain vertaa käyttäjän valitsemaa www-osoitetta tunnettujen haitallisten sivujen tietokantaan ja mikäli sivu löytyy listasta, selain estää pääsyn. Valitettavasti nämä suojaohjelmat eivät täysin aukottomasti pysty vaalimaan käyttäjiä vaarallisilta verkkosivuilta. Vaikka lista vaarallisista sivuista päivittyy koko ajan, ei kaikkia haitallisia sivuja voida mitenkään kartoittaa. Listan ulkopuolelle jää hurja määrä sivuja, jotka voivat silti sisältää haitallisia elementtejä. Täten selaimen sisäänrakennettuun suojaukseen ei voi täysin sokeasti luottaa. Lisäturvaa surffailuun voi hakea asentamalla esimerkiksi SiteAdvisor-nimisen lisäosan selaimeensa. Ohjelma toimii selaimen ohessa ja varoittaa käyttäjää epäluotettavista sivuista. (Järvinen 2012, 66 – 67.) Nettisurffailussa oman harkinnan ja järjen käyttö on paras tietoturva-ase ongelmia vastaan. Mikäli et ymmärrä kysymystä, älä klikkaa ok. Mikäli jokin näyttää epäilyttävältä tai oudolta, se yleensä on juuri sitä.

Verkkoselaimiin on saatavilla myös kosolti muita laajennuksia, jotka tuovat verkossa surffailuun lisäturvaa. Häiritsevien mainosten, ponnahdusikkunoiden ja muiden tarpeettomien ilmoitusten estämiseen kehitetyt laajennukset tekevät selailusta miellyttävämpää sekä myös turvallisempaa. Useimmiten erilaisia sivuja koristavat mainokset ovat vain ärsyttäviä ja sivuston selaamista hidastavia, mutta eivät varsinaisesti vaarallisia. Joissain tapauksissa kuitenkin haittaohjelmia on levitetty nimenomaan mainosten avulla. Täten mainosten estäminen on usein erittäin hyvä idea: se tekee www-sivujen käytöstä miellyttävämpää ja tukkii samalla yhden potentiaalisen tietoturva-aukon. Tällaisia mainosten ja muiden ilmoitusten estämiseen suunniteltuja laajennuksia ovat esimerkiksi AdBlock, Adblock Plus ja uBlock Origin.

Yksi käyttökelpoisimmista selainten ominaisuuksista on yksityistila. Käytetty termi vaihtelee eri selainten välillä, mutta yksityistilan perusperiaate on kaikissa sama. Yksityistilan ollessa päällä selaimeen ei jää jälkiä kyseisestä istunnosta. Näin käyttäjä voi selata verkkoa jättämättä selaimen sivuhistoriaan tai välimuistiin mitään tietoja. Esimerkiksi lainattaessa toisen konetta on hyvä käytäntö käyttää yksityistilaa, jotta esimerkiksi salasanoja ei vahingossakaan tallennu toisen henkilön koneelle. Vaikka yksityistila minimoi surffailun jättämän jäljen koneelle, ei se kuitenkaan estä esimerkiksi yrityksen tietohallintoa näkemästä mitä verkossa tapahtuu. Yksityistila ei siis tee itse verkon käytöstä anonyymia, vaan ainoastaan poistaa surffailun jäljet tietokoneelta. Näin samaa konetta käyttävät eivät voi urkkia aiempien istuntojen tallennettuja salasanoja tai sivuhistoriaa, sillä kaikki nämä ovat tipotiessään. Yksityistila itsessään ei takaa tietoturvaa, eikä se estä mahdollisia haittaohjelmia toimimasta ja kaappaamasta

tietoja. Yksityistila on hyvä esimerkki selainten tietoturvaa lisäävistä ominaisuuksista, sillä se turvaa käyttäjän yksityisyyttä ja estää parhaimmillaan kiusallisten tietoturvavahinkojen tapahtumisen. (Järvinen 2012, 76 – 77.)

4.4 Tietojenkalastelu

Tietojenkalastelu eli phishing tarkoittaa rikollista toimintaa jossa käyttäjiltä udellaan henkilökohtaisia tietoja. Henkilö- tai tilitietoja saatetaan tiedustella esimerkiksi houkutusviestein, jotka näyttävät pahaa-aavistamattoman käyttäjän silmiin hyvin paljon virallisten tahojen lähettämiltä yhteydenotoilta. (Andreasson 2013, 169.) Tietojenkalastelu tietoturvauhkana perustuu täysin käyttäjien hyväuskoisuuden hyväksikäyttöön. Huijarit pyrkivät saamaan uhrin luovuttamaan itse luottamukselliset tietonsa heille, jotta he voisivat sitten käyttää näitä tietoja rikollisiin tarkoituksiin. Tyypillinen kalasteluhuijaus on sähköposti, jossa on linkki väärennetylle www-sivulle. Tietojenkalasteluun ei kuitenkaan välttämättä tarvita edes tietokonetta, sillä tietoja voidaan kalastella myös puhelimitse tai tapaamalla kahden kesken (Järvinen 2006, 274). Tämän työn aihealueeseen kuitenkin olennaisesti kuuluu nimenomaan tietojenkalastelu sähköpostin ja www-sivujen avulla.

Ihmisiä varoitellaan toistuvasti pankkien ja uutissivustojen toimesta rikollisten kalasteluyrityksistä. Kaikesta tästä valistuksesta ja muistuttelusta huolimatta valitettavan useat huijausyritykset onnistuvat silti. Huijareiden viestit saattavat olla hyvin virallisen oloisia ja sivut saattavat olla identtisiä virallisten sivujen kanssa. Tämä tekee huijausviestien tunnistamisesta haasteellista, mikäli ei tiedä mihin seikkoihin tulisi kiinnittää huomiota.

Tyypillinen sähköpostilla tapahtuva tietojenkalastelu alkaa sähköpostiviestillä, jossa huijauksen uhrille esitetään jokin tekosyy, jonka vuoksi tähän ollaan yhteydessä sähköpostitse. Yleensä houkuttimena toimii luottokortin loppuminen, tietojen päivitys tai kenties murtoyritysten sarja joka olisi kohdistunut käyttäjän tiliin. Sähköpostiviesti ohjaa huijattavan linkin kautta www-sivulle, joka näyttää identtiseltä oikean palvelun kanssa, mutta on oikeasti huijaussivusto. Pahimmassa tapauksessa uhri ”kirjautuu” palveluun sisään ja syöttää pyydetyt tiedot, antaen samalla rikollisille liudan henkilökohtaisia tietojaan. (Järvinen 2012, 73.)

Miten sitten tunnistaa mahdollinen tietojenkalasteluyritys? Nyrkkisääntönä voisi pitää sitä, että pankit ja maksupalvelut eivät lähesty käyttäjiään sähköpostin välityksellä. Pankit eivät koskaan tiedustele käyttäjiensä kirjautumiskoodeja. Usein viestit on kirjoitettu ontuvalla suomen kielellä, sillä käännöstyöhön on saatettu käyttää käännöskonetta. Tämän tulisi ainakin herättää käyttäjän epäilykset. (Järvinen 2006, 286 – 287.)

Mikäli epäilee joutuneensa huijaussivulle, on syytä kiinnittää huomiota jo aiemmin tässä työssä esitettyihin seikkoihin. Onko sivun varmenne kunnossa? Käyttääkö sivu SSL-salausta? Alkaahan osoitekentässä oleva osoite kirjaimilla

HTTPS? Varmenteen ja salauksen puuttuminen virallisten tahojen sivuilta on merkki huijauksesta. Tärkeää on tarkistaa aina luottamuksellisia tietoja liikuttaessa, että SSL-tekniikka on käytössä. Mikäli salaus on käytössä, selaimessa näkyy lukon kuva ja osoiterivi alkaa kirjaimilla HTTPS. Selaimen varoittaessa epäluotettavasta varmenteesta sivulla, joka ennen on toiminut moitteettomasti voi kyse olla huijauksesta. Jos virheilmoitus tapahtuu jokaiselle SSL-suojatulle sivulle pyrkiessä, vika voi olla myös oman koneen väärässä kalenterivuodessa. Tärkeintä on kiinnittää huomio selaimen osoitekenttään. Mikäli osoitekentässä oleva URL, www-sivun osoite, ei ole sama kuin tavallisesti palvelua käytettäessä kyse voi olla huijaussivusta. Viisasta on tallentaa käyttämänsä palvelut selaimen kirjanmerkkeihin ja avata sieltä tai kirjoittaa osoite aina itse osoitekenttään. Näin voi varmistua osaltaan käyttävänsä oikeaa sivustoa. Sähköpostista palveluiden linkkien availeminen ei ole viisasta. Jos sivu vaikuttaa epäilyttävältä, voi aina kokeilla kirjautua sisään väärillä tunnuksilla. Mikäli kirjautuminen vaikuttaa onnistuvan värilläkin tiedoilla ja sivusto silti laskee käyttäjän sisään, on syytä epäillä kyseessä olevan rikollisten kalastelusivusto. (Järvinen 2012, 73 – 75.)

Tärkeintä on muistaa ja ymmärtää, että suomalaiset pankkipalvelut eivät koskaan lähesty käyttäjiään sähköpostitse. Jos sähköpostiviestissä kehoitetaan kirjautumaan sisään palveluun sähköpostilinkin kautta, kyse on huijauksesta. Oikea palvelu kysyy pelkästään yhtä kirjautumiskoodia. Useampaa salasanaa tai koodia kysyvä palvelu on kalasteluhuiputus. (Järvinen 2012, 74 – 75.)

5 HAITTAOHJELMAT

Haittaohjelma (malware) on yleisnimitys kaikille ohjelmille, jotka koneelle päästessään aiheuttavat käyttäjälle harmia tai suoranaista vahinkoa. Haittaohjelmia on monta erilaista tyyppiä, jotka kaikki tarttuvat erilaisin keinoin. (Järvinen 2006, 77.) Yhdistävä tekijä näille ohjelmille on lähinnä vain se, että kaikki nämä johtavat ei-toivottuihin muutoksiin tietokoneessa ja lopputulema on usein käyttäjän kannalta hyvin epäsuotuisa.

Haittaohjelmien historia tietokoneita vaivaavana kiusankappaleena on melko pitkä, mutta niiden muodostama uhka ja levinneisyys ovat aivan toista maata kuin 80-luvulla. Haittaohjelmien historian alkuvaiheilla viruksia ja matoja kyhäilivät lähinnä nuoret tietokoneharrastelijat, jotka saivat tyydytystä leikkiessään lainsuojattomia. Haittaohjelmien koodaaminen yömyöhään monitorin kajastuksessa palkittiin vain muiden harrastelijoiden osoittamalla kateudensekaisella ihastuksella ja kunnialla. Ajan myötä haittaohjelmien tehtailu on muuttunut harrastelijoiden huvista järjestäytyneen rikollisuuden toimintaan, jonka tavoitteena on saavuttaa taloudellista hyötyä. Tavanomaisten käyttäjien vallatessa netin on myös rikollinen toiminta seurannut perässä. Näin haittaohjelmien teko on muuttunut bisnekseksi, jossa huomaamattomimman ja vaarallisimman haittaohjelman tekijälle rikolliset syytävät rahaa. Haittaohjelmien teosta on tullut ammattimaista toimintaa ja ohjelmista sen myötä entistä vaarallisempia. (Järvinen 2006, 77.)

Pelottava esimerkki uudenaikaisista, taloudellista hyötyä rikollisille tavoittelevista haittaohjelmista on pankkitroijalainen. Tämä on varsin ikävä haittaohjelma, sillä se manipuloi pahaa aavistamattoman uhrin konetta siirtämällä uhrin tililtä rahaa ulkomaisille tileille käyttäjän huomaamatta (Järvinen 2012, 64). Katastrofi paljastuu käyttäjälle usein vasta tiliotteen kolahtaessa postilaatikkoon. Mikäli ennen tietokoneharrastelijoiden alkeellisten virusten ja matojen tarkoitus oli lähinnä kerätä tekijälleen kunniaa ja aiheuttaa haittaa jonka käyttäjä pystyy helposti huomaamaan, on modernien haittaohjelmien toimintaperiaate täysin päinvastainen. Rikollisten toiminnan kannalta parasta on pysyä piilossa. Mikäli käyttäjä ei edes huomaa haittaohjelman mellastavan koneella ja torjuntaohjelmat eivät hälytä, pääsee haittaohjelma tekemään tehtäväänsä kaikessa rauhassa. Näin pahantekijät pääsevät mahdollisesti nauttimaan työnsä hedelmistä mahdollisimman kauan, haittaohjelman jatkaessa toimintaansa huomaamatta. Yksi vaarallisimmista, ja samalla rikollisten keskuudessa kysytyimmistä, haittaohjelmista on jokin sellainen ohjelma joka hyödyntää ns. nollapäivähaavoittuvuutta. Nollapäivähaavoittuvuudella tarkoitetaan tietoturva-aukkoa, joka ei ole vielä suuren yleisön tiedossa ja on täten korjaamaton. Pimeillä markkinoilla tällaisesta nollapäivähaavoittuvuudesta voidaan pulittaa jopa miljoona dollaria. (Järvinen 2012, 183.)

Tavanomaisesti on tuudittauduttu ajatukseen, että haittaohjelmat leviävät pääasiassa käyttöjärjestelmien ja sovellusten tietoturva-aukkoja hyväksikäyttäen. Tietokoneiden ja muiden laitteiden käyttö on muuttunut merkittävästi paikalli-

sesta koneella työskentelystä erinäköisten verkkopalveluiden käyttöön. Rikolliset muuntavat toimintaansa tavanomaisten käyttäjien toiminnan mukaan ja pyrkivät aina olemaan siellä missä heidän potentiaaliset pahaa-aavistamattomat uhrinsakin. Täten myös haittaohjelmat ovat siirtyneet hyödyntämään myös erilaisia verkon palveluita, kuten vaikkapa Facebookia. Vaaralliset ohjelmat voivat levitä jopa kyseisen palvelun tai selaimen sisällä. (Järvinen 2012, 180.) Haittaohjelmat leviävät useita erilaisia kanavia pitkin. Ne tavanomaisesti hyödyntävät joko ihmisten paljon käyttämiä palveluita (esim. sähköposti) tai sitten käyttävät häikäilemättömästi hyödykseen joitain järjestelmien tunnettuja tietoturva-aukkoja.

Klassinen esimerkki ja ikuisen tietoturvakoulutuksen aihe on vaarallisten ohjelmien leviäminen sähköpostin välityksellä. Vaikka ansiokas tietoturvakoulutus on tehnyt käyttäjistä valppaampia ja varovaisempia outojen liitetiedostojen suhteen, toisinaan kuitenkin joku käyttäjistä haksahtaa avaamaan tällaisen tiedoston. Kyseessä voi olla laskuksi naamioitu haittaohjelma, tai kenties jonkinlainen palkkakuitti joka lataa koneelle haittaohjelman paikkaamattoman tietoturva-aukon kautta. Sähköpostin kautta voi tulla myös linkki vaaralliselle sivulle, jossa käyttäjää kehoitetaan lataamaan ohjelma tai antamaan arkaluontoisia tietoja tietojenkalastelusivulle. Usein sähköpostien omat torjuntaohjelmat ovat sen verran kehittyneitä, että ne tunnistavat tällaiset epäilyttävät viestit ja pystyvät varoittamaan käyttäjää vaarasta. Kaikki torjuntamekanismit ovat erehtyväisiä, joten käyttäjän on myös itse syytä kyetä tunnistamaan epäilyttävät sähköpostit. (Järvinen 2012, 181 – 182.) Tiedostopäätteet ovat hyvä keino tunnistaa tiedoston käyttötarkoitus. Mikäli ei ole täysin varma tiedoston turvallisuudesta, kannattaa eritoten sellaisiin tiedostoihin jotka päättyvät .exe, .scr tai .vbs päätteeseen suhtautua varovaisuudella. Windows-käyttöjärjestelmissä tiedostopäätteet eivät näy oletusarvoisesti käyttäjälle, mikä hankaloittaa tiedostojen tunnistusta. Tämän voi kuitenkin muuttaa ohjauspaneelissa sijaitsevasta kansion asetukset valikosta poistamalla valinnan kohdasta piilota tunnettujen tiedostotyyppien tunnisteet. Näin tiedostopääte saadaan luettavaksi tiedostonimen perästä ja epäilyttävien tiedostotyyppien tunnistaminen helpottuu.

Toinen yleinen tapa, jolla virukset ja haittaohjelmat leviävät, on www-sivustojen kautta. Tämän vuoksi olisi ensiarvoisen tärkeää päivittää oma verkkoselaimensa ja pysyä poissa niiltä internetin epämääräisimmiltä sivuilta. Joskus suurinkaan varovaisuus ei riitä, sillä toisinaan on käynyt niin että hyvämaineisetkin sivut ovat saattaneet tartuttaa käyttäjiä. Rikollinen taho on saattanut tietomurron yhteydessä istuttaa ohjelmansa sivulle, tai haittaohjelma leviää mainosten kautta joista vastuussa on yleensä ulkopuolinen taho. Käyttäjä itse voi päivittää selaimensa, päivittää oheisohjelmat ja poistaa tarpeettomat lisäosat. (Järvinen 2006, 80 – 81.) Verkkosivuista eritoten vaarallisimpia ovat kaikenlaiset piraatti- ja warez-sivut, joilla on kaikenlaista kyseenalaista ja jossain määrin jopa laitonta sisältöä. Vaarallisiksi ovat osoittautuneet myös videopelien huijaus- ja aktivointikoodeja sisältävät sivut.

Tarpeellista lienee vielä mainita USB-tikut haittaohjelmien levityksen kanavana. Moni survaisisi kadulta löytämänsä satunnaisen USB-tikun asiaa sen

kummemmin pohtimatta koneeseen kiinni, mutta kyse saattaa olla ilkeämielisen tahon virittämästä ansasta. Tikkujen avulla haittaohjelmat pääsevät tarttumaan hyvinkin suojattuihin koneisiin, joihin ei välttämättä ole pääsyä edes julkisesta verkosta. Ei ole tavatonta, että hyvin suojatun tehtaan tietojärjestelmiä on päässyt vaivaamaan haittaohjelma, kun tietoturvaohjeista piittaamaton työntekijä on kytkenyt saastuneen USB-tikun työpaikan tietokoneeseen kiinni. Hyökkääjä on saattanut esimerkiksi asettaa tikun tarkoituksella työntekijän löydettäväksi, jotta pääsisi käsiksi tämän yrityksen tietoihin tikulla sijaitsevan haittaohjelman avulla. (Järvinen 2012, 188.)

Haittaohjelmista uutisoidaan usein tiedotusvälineissä, mutta niistä käytävä keskustelu vilisee mitä kummallisempia termejä joita asiaan vihkiytymättömän henkilön lienee haasteellista ymmärtää. Totta on, että haittaohjelmien kirjo on niin laaja, että niistä muodostuu väistämättä varsin tiheä käsiteviidakko josta on joskus hankala saada tolkkua. Haittaohjelmien nimeäminen ja jaottelu usein on varsin suoraviivaista, pohjaututuen periaatteessa siihen mitä kukin ohjelma tekee. Jaottelu tapahtuu sen perusteella, miten haittaohjelma leviää, miten se toimii tai mitkä sen vaikutukset ympäristölle ovat. Nimensä mukaisesti kuitenkin kaikki haittaohjelmat ovat vaikutuksiltaan käyttäjälle haitallisia, aina harmillisen kiusallisista katastrofaalisen tuhoisiin asti.

Seuraavaksi esitellään muutamia yleisimpiä haittaohjelmia ja niihin liittyviä käsitteitä.

5.1 Mato

Madot levittyvät itse itseään kopioimalla koneesta toiseen hyödyntäen käyttöjärjestelmän tai sovellusten tietoturva-aukkoja. Vaikkakin madot vaikutuksiltaan ovat usein korkeintaan harmillisia ja vähemmän vahingollisia, saattaa matojen leviäminen tukkia verkot sekä siinä kiinni olevat laitteet. Matojen aika alkaa kuitenkin olla ohi. Haittaohjelmilla bisnestä tekevien rikollisten tarpeisiin madoilla ei voi tehdä tarpeeksi vahinkoa, joten madoilla ei juuri ole arvoa haittaohjelmien markkinoilla. Samalla myös palomuurit ja käyttöjärjestelmien päivittäminen ovat yleistyneet ja tukkivat madoilta yleisimmät aukot joita pitkin luikerrella sisään tietokoneisiin. (Järvinen 2006, 88.)

5.2 Virus

Tietokonemaailman virukset leviävät usein selaimen tai sähköpostin liitetiedostojen välityksellä. Mahdollista on myös, että virus tarttuu usb-tikkujen, cd-levyjen tai muiden tiedontallennusvälineiden avulla koneesta toiseen. Tämän vuoksi olisi syytä välttää tuntemattomien usb-muistien kytkemistä koneeseen ja jättää avaamatta epäilyttävät sähköpostiliitteet. Tyypillisesti viruksen päästyä koneelle se pyrkii näkymättömissä levittämään itsestään kopioita mahdollisimman laajalle, saastuttaen koneeseen kytketyt tiedontallennusvälineet sekä itse koko tietokoneen. Tämän jälkeen virus ryhtyy varsinaiseen tuhotyöhön.

Yleensä tässä vaiheessa virus ryhtyy hävittämään kiintolevyltä tietoja tyhjentämällä levyn tilanvaraustaulukon. Tiedot näyttävät kadonneen ja käyttäjä hätääntyy. Tällaisessa tapauksessa kuitenkin tiedot saattavat olla pelastettavissa apuohjelmalla, sillä tiedot eivät varsinaisesti ole hävinneet minnekään. Virus on ainoastaan tyhjentänyt tilanvaraustaulukon ja tietokone ei täten tunnista tietojen olevan levyllä. Toinen, ilkeämpi vaihtoehto on, että virus kirjoittaa aktivoiduttuaan kiintolevylle roskakoodia, saastuttaen samalla kaikki koneen tiedostot. Tietojen pelastamisesta ei ole toivoa, sillä saastuneet tiedostot ovat käyttökelvottomia. (Suomen Internetopas 2016.)

5.3 Troijalainen

Troijalaisella tarkoitetaan yleensä ohjelmaa, joka vaikuttaa käyttäjän silmissä hyödylliseltä, mutta samalla tekee haittaohjelmalle tyypillisiä tehtäviä aiheuttaen käyttäjälle harmia ja kiusaa. Sana troijalainen juontaa juurensa kreikkalaisesta mytologiasta, jossa kreikkalaiset pääsivät piirittämänsä Troijan kaupungin sisäpuolelle piiloutuen suuren puuhevosen sisään. Usein tietokonemaailman troijalainen toimii samoin, esiintyen hyödyllisenä ohjelmana, avaten samalla haittaohjelmille aukon tietokoneelle jotta nämä pääsisivät aiheuttamaan lisää tuhoa. Madoista ja viruksista poiketen troijalainen ei pyri levittymään eteenpäin, vaan troijalainen pyrkii toimimaan mahdollisimman huomaamattomasti. (Järvinen 2012, 178.)

Esimerkki pelottavasta ja erittäin kehittyneestä troijalaisesta on jo tässä työssä aiemmin mainittu pankkitroijalainen. Pankkitroijalaisten kehitystyön keskus sijaitsee Itä-Euroopassa, josta rikolliset tahot voivat niin halutessaan lunastaa pankkitroijalaisen yleisohjelman ja ohjeet joiden avulla tämä kohdennetaan juuri kyseisten roistojen haluamalle pankkipalvelulle. Nämä ohjelmat kun useimmiten kohdennetaan toimimaan tietyn pankin palvelun kanssa. Tässä tapauksessa Suomi hyötyy pienuudestaan, sillä rikollisiin tarkoituksiin räätälöity ohjelma kannattaa ennemmin päästää valloilleen maassa jossa pankkiohjelmilla on paljon käyttäjiä. Pankkitroijalaiset ovat esimerkki siitä, miten vaarallisia ja kehittyneitä jotkin troijalaiset ovat. Pankkitroijalaisen toimiessa taustalla yhteys näyttää käyttäjälle ja pankille turvalliselta, mutta yhteyden eheys on murrettu sillä haittaohjelma manipuloi käyttäjän tekemiä rahansiirtoja. Kaikki näyttää käyttäjän puolesta toimivan oikein, sillä troijalainen muuntelee pankkiohjelman näyttöä peittääkseen jälkensä. Koko ajan kuitenkin haittaohjelma lisää tilisiirtoja käyttäjän tililtä ulkomaille. Käyttäjän tietoon rahojen katoaminen tulee usein vasta tiliotteen saapuessa kotiin tai sähköpostiin. (Järvinen 2012, 64.)

5.4 Takaovi

Rikollinen taho on saattanut lisätä sinällään hyödylliseen ohjelmaan salaisen takaoven, jonka kautta tämä ulkopuolinen taho voi päästä käsiksi uhrin koneeseen ja ottaa laitteen haltuunsa (Järvinen 2012, 179). Takaoven kautta ulkopuo-

linen taho voi tutkiskella koneella olevia yksityisiä tietoja, sekä kopioida, muokata ja tuhota tiedostoja. Takaoven kautta rikollinen voi seurata tietokoneella työskentelyä ja ottaa halutessaan kuvaruutukaappauksia toiminnasta. Pahantekijät ovat usein myös käyttäneet koneelle ujuttamaansa takaovea kuvatakseen koneiden käyttäjistä arkaluontoisia kuvia tietokoneen omaa kameraa käyttäen. Useimmiten takaovi avautuu koneelle osana toisen tai useamman haittaohjelman toimintaa koneella. (Viestintävirasto 2015.)

5.5 Bottiverkko

Bottiverkko koostuu tietokoneista, jotka rikollinen taho on saanut haltuunsa esimerkiksi troijalaisen tai takaoven avulla. Saastunut kone on haltuunoton jälkeen liitetty rikollisen toimesta osaksi muiden saastuneiden koneiden verkkoa, joita rikolliset sitten käyttävät suorittaakseen verkkorikollisuuteen liitettäviä tehtäviä. (Järvinen 2006, 88 – 89.) Vieraiden saastuneiden koneiden armeijaa hallitsevat tahot myyvät palveluita eteenpäin muille rikollisille, jotka saattavat tarvita tuhansien tietokoneiden verkostoa esimerkiksi palvelunestohyökkäyksen luomiseksi. Ilkeämielinen taho valjastaa kaikki hallussaan olevat koneet pommittamaan estetyksi haluttua palvelua turhalla liikenteellä, jotta palvelu hukkuisi liiallisen kuorman alle. Bottiverkkoa saatetaan myös käyttää esimerkiksi massiivisen roskapostitulvan lähettämiseen, salasanojen murtamiseen tai bittirahan louhimiseen. Tuhansien laitteiden verkkoa saatetaan myös käyttää tietomurtojen jälkien peittämiseen, sillä useiden kymmenien tuhansien laitteiden joukosta on hankala sanoa, kuka on todellisuudessa vastuussa hakkeroinnista. (Järvinen 2012, 179.)

Käyttäjä ei toisinaan edes huomaa koneensa olevan osa bottiverkkoa. Ainoat merkit tästä ovat koneen hidastuminen ja verkkoliikenteen kasvu, mutta toisaalta näin voi käydä vaikka kone ei edes olisi osa bottiverkkoa. Useimmiten asia paljastuu vasta, kun palveluntarjoaja ilmoittaa bottiverkon pesiytyneen heidän verkkoonsa tai sulkee tietokoneenomistajan nettiliittymän. (Järvinen 2012, 179.)

5.6 Näppäimistökaappari

Näppäimistökaappari (keylogger) urkkii käyttäjän näppäimistön painalluksia, tallentaen toimiessaan käyttäjän salasanat, tunnukset ja arkaluontoiset keskustelut. Edistyneemmät ohjelmat saattavat myös ottaa kuvakaappauksia tietokoneen näytöltä tasaisin väliajoin. Kaappari voi olla ohjelma koneella, tai fyysinen lisälaite tietokoneen ja näppäimistön välissä jonka hakkeri on sinne asentanut. Fyysisen näppäinkaapparin muistiin mahtuu n. puoli miljoonaa painallusta ja se tallentaa myös järjestelmän kirjautumistunnukset ja mahdolliset lähiverkon salasanat. Kaiken. Tiedot tallentuvat kaapparin omaan muistiin ja urkkija käy noutamassa kaapparin koneesta aikanaan tutkiakseen sen keräämän datan. Ohjelmapohjainen kaappari taasen lähettää tietoja eteenpäin, esimerkiksi sähköpostilla. (Järvinen 2012, 129.)

Vaikka kertakäyttötunnukset ovat tehneet pankkitunnusten urkkimisesta vaikeaa, ovat jotkin näppäimistökaapparit hyvin kehittyneitä ja kykeneväisiä muuttamaan mm. tilisiirtoja. Käyttäjän maksaessa laskua tilisiirron kohteeksi muuttuukin huomaamatta rikollisen tahon tili ja rahat siirtyvät rikolliselle käyttäjän haluaman tahon sijaan. (Järvinen 2006, 89.)

5.7 Kaikenlaista warea – mitä ihmettä ne tarkoittavat?

Yleinen tietoturvakeskustelu ja uutisointi ovat täynnä mitä kummallisempia nimityksiä ja termejä. Usein suomenkielisen tekstin sekaan on ujutettu vierasperäisiltä kuulostavia termejä, joita toisinaan lukijan saattaa olla hankala tulkita. Sanoille löytyisi useimmiten selkokielinen suomenkielinenkin vastine. Käytetyn kielen englannistuminen ja yleinen rappeutuminen ovat kuitenkin johtamassa siihen, että keskustelupalstoilla ja uutisoinnissa otetaan usein vapauksia hyvän suomen kielen kustannuksella. Käytetyt termit johdetaan suoraan englannin kielestä, eikä kirjoitettaessa välttämättä käytetä niiden helpommin ymmärrettäviä supisuomalaisia vastineita. Tämä hankaloittaa keskustelujen, ohjeiden ja uutisten ymmärtämistä. Tietoturvaan liittyvä keskustelu pitää sisällään kaikenlaisia ware-päätteisiä termejä. Tämä ei kuitenkaan tarkoita sitä, että pitäisi pelästyä nähdessään sanaan ware loppuvan englanninkielisen termin jossain. Ware-päätettä käytetään varsin yleisesti englannin kielessä kuvaamaan tietokoneisiin liittyviä asioita, ohjelmia tai vaikkapa komponentteja. Seuraavassa esitellään muutamia esimerkkejä erilaisista haittaohjelmista ja niihin liittyvistä termeistä.

Yleisnimitys kaikille haittaohjelmille on malware (Järvinen 2006, 77). Kuten olemme jo todenneet, haittaohjelmia on kuitenkin hyvin monenlaisia. Näin insinööreille on ilmestynyt tarve pystyä paremmin luokittelemaan näitä ohjelmia, sillä pelkkä haittaohjelman käsite on varsin laaja ja ongelmallisten ohjelmien kirjo niin laaja. Kyseessä voi olla kiusallinen mainosohjelma (adware), joka täyttää tietokoneen mainoksilla tai aggressiivinen rahan varastamiseen (stealware) keskittyvä ohjelma (Järvinen 2006, 80). Vakoiluohjelma (spyware) taasen kerää käyttäjän yksityisiä tietoja ja levittää niitä eteenpäin ilman käyttäjän antamaa suostumusta (Järvinen 2006, 80). Haittaohjelmien skaala on laaja.

Viime aikoina julkisuudessa on paljon varoiteltu kiristyshaittaohjelmista (ransomware). Yleensä tällaiset ohjelmat toimivat siten, että saastuneen koneen käyttäjä saa ilmoituksen jossa kerrotaan käyttäjälle paikallisen viranomaisen lukinneen tietokoneen. Käyttäjää saatetaan syyttää jonkinlaisesta rikoksesta. Haittaohjelma kuitenkin ilmoittaa käyttäjälle, että 100-150 euron sakon kuittaamalla kone aukeaa jälleen. Oikeat viranomaisethan eivät koskaan lukitse tietokoneita tai esitä sakkovaatimuksia internetin välityksellä. Haittaohjelma tekee tietokoneen tiedostoista käyttökelvottomia salaamalla ne. Salaus on usein niin vahva, että tiedostoja ei saada koskaan palautettua takaisin. Lunnaiden maksaminen ei takaa tiedostojen palauttamista ja ainoastaan tukee rikollisten

tahojen toimintaa entisestään. Tämän vuoksi tärkeistä tiedostoista tulisi ehdottomasti löytyä varmuuskopiot. Yleisimpiä tällaisia kiristyshaittaohjelmia ovat CryptoWall ja TorrentLocker. (Poliisi, CERT-FI ja F-Secure Oy 2016.)

Pelotteluohjelmat (scareware) ovat huijausohjelmia, jotka mainostavat näyttävästi korjaavansa tietokoneen ongelmia tai nopeuttavansa koneen toimintaa merkittävästi. Tällaisia mainoksia saattaa löytyä jopa luotettavien sivustojen, esimerkiksi suosittujen uutissivustojen lööppien välistä. Mainos saattaa houkutella käyttäjää tarkistamaan tietokoneen mahdollisten ongelmien varalta, tai lataamaan ohjelman joka nopeuttaa konetta 150-kertaisesti. Nämä ohjelmat eroavat asiallisista, oikeista tietokoneen apuohjelmista siten, että huijausohjelmat löytävät aina koneelta virheitä tai haittaohjelmia vaikka niitä ei olisikaan. Virheiden korjaamiseksi ohjelma vaatii käyttäjältä rahaa. Kyseiset huijausohjelmat ovat tekijöilleen hyvin tuottoisia, sillä lankaan menneitä ihmisiä on paljon. Täten ohjelmien kehittämiseen käytetään paljon aikaa ja ohjelmat näyttävät hyvin ammattimaisesti tehdyiltä. Huijauksen tunnistaminen voi olla haasteellista. Parasta on pitäytyä luotettaviksi tiedetyissä ohjelmissa. Nopea tiedonhaku Googlella ja keskustelupalstojen mielipiteiden vilkaiseminen paljastaa usein onko kyse asiallisesta toimijasta vai valeohjelmasta. (Järvinen 2012, 213 – 217.)

6 KONEEN TURVALLISUUDEN KOHENTAMINEN

Tärkeä osa oman tietoturvan ylläpitoa on omien laitteiden – tietokoneiden, puhelimien, tablettien – turvallisuuden takaaminen. Jotta voisi turvallisin mielin hoitaa asioitaan netissä ja säilöä tärkeitä tietoja koneelleen, pitää käyttäjän tehdä voitavansa jotta tietokoneen perustava turvataso olisi kunnossa. Kuten työssä on jo aiemmin esitelty, erilaisia uhkia kotikoneen tietoturvalle on monia. Tietokoneella käytetyt ohjelmat saattavat sisältää tietoturva-aukkoja tai käyttäjä voi tulla huiputetuksi ja avata itse sellaisen. Koneella ei välttämättä tarvitse edes olla haittaohjelmaa, sillä inhimillinen virhe käyttäjän toimesta saattaa johtaa tietojen vuotamiseen tietojenkalastelijalle. Kysymys onkin, miten käyttäjä voi suojata kotikoneensa tärkeät tiedostot, turvata omat tietonsa ja tukkia tietoturva-aukot kun kaikenlaisia uhkia on niin monia? Aiemmissa luvuissa esitettyjen ohjeiden lisäksi tärkeä osa tätä prosessia on oman koneen tietoturvan asiallinen hoitaminen. Vaikka oman henkilökohtaisen tietokoneen tietoturvaohjelmistojen ja päivitysten asentaminen saattaa useimmista kuulostaa varsin tekniseltä, monimutkaiselta tai vähintäänkin sitten vain kuolettavan tylsältä, on kyse kuitenkin olennaisista toimenpiteistä koneen tietoturvan varmistamiseksi. Vastuu omasta tietoturvasta on lopulta yksilöllä itsellään ja tietoturvaan liittyvät vaatimukset eivät tule nykyisessä tietoyhteiskunnassa ainakaan vähenemään. Siksi olisi erittäin tärkeää, että kaikilla olisi perustavaa laatua oleva käsitys siitä miten oman henkilökohtaisen tietokoneen tietoturva pyritään varmistamaan.

Kuten kaikessa muussakin, myös tietokoneen tietoturvan osalta voidaan sanoa, että hankala on onnistua jos perusteet eivät ole kunnossa. Oman koneen tietoturvan osalta tärkeää on, että perustavaa laatua olevat ohjelmat ja käytännöt ovat olemassa, jotta tietokoneen turvallinen käyttö voisi onnistua. Mikään määrä tietoturvakoulutusta ja hyviä salasanoja ei korvaa näitä. Tietokoneen tietoturvan osalta puhutaan paljon erilaisista palomuureista ja virustorjunnoista, eikä syyttä. Markkinoilta löytyy paljon helppokäyttöisiä, hyviä ohjelmia joiden käyttämiseen ei ole tarvinnut lukea itseään tietotekniikan insinööriksi. Palomuuri ja virustorjunta ovat olennaisia työkaluja taistelussa haittaohjelmia ja tunkeilijoita vastaan. Koko tietokoneen toiminta perustuu käyttöjärjestelmälle. Tämä toisaalta tekee siitä myös kiinnostavan kohteen rikollisille, sillä mahdollinen tietoturva-aukko käyttöjärjestelmässä avaisi rikollisille pääsyn lukemattomiin koneisiin. Tämän vuoksi on erityisen olennaista pitää käyttöjärjestelmä ajan tasalla päivitysten avulla. Olennaista on myös siirtyä vanhoista käyttöjärjestelmistä uusiin, kun vanhan järjestelmän tuki loppuu.

Langattomat nettiyhteydet ovat tuoneet myös uusia ongelmia tietokoneiden turvallisuudelle. Varsinkin julkisissa tiloissa tarjotut avoimet ja ilmaiset verkot ovat ongelmallisia, sillä niitä voi käyttää kuka tahansa. Täten verkkoa saattaa käyttää myös pahansuopa henkilö, joka seuraa muiden käyttäjien tekemisiä poimien verkkoliikenteestä salasanoja, käyttäjätunnuksia sekä muita tietoja. Myös oman kotiverkon turvaaminen salasanalla ja salauksella on täten tärkeää. Mikäli verkkoa ei ole suojattu salasanalla on kuka tahansa sitä tervetullut käyttämään. Suomen laki määrittelee, että mikäli esimerkiksi naapurin nettiä ei ole

suojattu salasanalla, voi sitä toinen naapuri käyttää ilman omistajan lupaa (Viestintävirasto 2014).

Toisinaan katastrofi kuitenkin tapahtuu, eikä mitään ole tehtävissä. Näissä tilanteissa varmuuskopiointi voi osoittautua kultaakin kalliimmaksi. Osa tärkeiden tiedostojen vastuullista käsittelyä on varautua kaikista pahimpaan ja tehdä niistä kopioita hyvissä ajoin. Jos käytäntö on mitään osoittanut niin sen, että ikinä tietokoneen kiintolevyn hajoamiselle, mahdolliselle haittaohjelmien invaasiolle tai tietokoneen mukanaan vieneelle tulipalolle ei ole sopivaa aikaa. Kalenteri ei käyttäjälle kerro, koska tiedot hävittävä katastrofi tulee tapahtumaan joten siihen on vain varauduttava järkevästi etukäteen. Paras aika toimia onkin nyt heti, mikäli tietokoneelta löytyy jotain minkä katoaminen ikuisiksi ajoiksi tuottaisi harmaita hiuksia.

6.1 Käyttöjärjestelmä

Käyttöjärjestelmä on olennaisin ja tärkein osa tietokoneen toimintaa. Toimiva käyttöjärjestelmä toimii perustana ohjelmien ja erilaisten palveluiden toiminnalle. Näin olennaisena osana kaikkien tietokoneiden toimintaa käyttöjärjestelmät ovat erityisen kiinnostavia kohteita rikollisten toiminnalle. Täten mahdolliset tietoturva-aukot ja virheet käyttöjärjestelmässä ovat äärimmäisen katastrofaalisia, sillä ne avaavat rikollisille potentiaalisen aukon miljooniin tietokoneisiin ympäri maailman. Synkkä tosiasia kuitenkin on se, että mikään käyttöjärjestelmä tai ohjelma ei ole täydellinen ja näiden valmistusprosessissa valmiiseen tuotteeseen jää aina aukkoja joita pitää myöhemmin korjata. Kysymys on vain siitä, kuka aukot huomaa ensimmäisenä ja ehditäänkö päivityksellä paikata virhe ajoissa. Päivitykset ovat virheiden, aukkojen tai puutteiden korjauksia valmiiseen ohjelmaan. Tämän vuoksi ohjelmien ja käyttöjärjestelmien päivittäminen on ensiarvoisen tärkeää. (Järvinen 2006, 16.)

Käyttöjärjestelmien päivitykset sisältävät usein tärkeitä tietoturvapaikkauksia jotka mahdollistavat koneen turvallisen käytön jatkumisen. Täten vanhojen käyttöjärjestelmien käyttäminen päivittäisessä toiminnassa on merkittävä tietoturvariski. Virallisen tuen päätyttyä vanhat käyttöjärjestelmät muodostuvat kiinnostavaksi kohteeksi rikollisille, sillä virallisten tietoturvapäivitysten tarjoaminen vanhoille järjestelmille loppuu. Tämä asettaa käyttäjät riskiryhmään, sillä minkäänlaisia päivityksiä ei ole luvassa vanhoille järjestelmille. Viimeaikojen merkittävin esimerkki tällaisesta tilanteesta on Microsoftin päätös lopettaa Windows XP-käyttöjärjestelmän tukeminen 8.4.2014 jälkeen. Tietoturvan ollessa jatkuvaa kilpailua turva-aukkoja hamuavien rikollisten ja päivityksistä, korjauksista sekä valistuksesta vastaavien tahojen välillä käytännössä käyttäjälle ei jää muuta vaihtoehtoa, kuin päivittää vanha käyttöjärjestelmä sellaiseen jossa valmistajan tuki on vielä voimassa. Tuen loputtua alkaa rikollisten tahojen ylivalta ja he saavat vapaasti hyväksikäyttää uusia löytämiään aukkoja ilman minkään virallisen tahon puuttumista asiaan. (Rousku 2014, 258.)

Windows Update on Microsoftin tarjoama työkalu uusimpien Windows-käyttöjärjestelmien päivittämiseen. Windows Updaten avulla käyttäjä voi tarkistaa onko saatavilla uusia päivityksiä ja hallita useita päivityksiin liittyviä asetuksia. Käyttäjän päätettävissä on suorittaako ohjelma itse päivitykset automaattisesti, vai tapahtuuko päivitysten lataus ja asennus vasta käyttäjän komennosta. Suositus on asettaa päivitykset tapahtumaan automaattisesti. Täten Windows Update lataa ja asentaa päivitykset ilman käyttäjän antamaa käskyä. Näin tärkeät päivitykset asentuvat hetimmiten. Mikäli käyttäjä haluaa itse päättää asennetuista päivityksistä, ottaa käyttäjä myös samalla kontolleen suuren vastuun muistaa asentaa päivitykset ajallaan. Tavallisille kotikäyttöön tarkoitetuille Windows-koneille on suositeltavaa asettaa päivitysten lataaminen ja asennus automaattiseksi toimenpiteeksi. (Rousku 2014, 260.)

Säännöllisten päivitysten lisäksi toinen erinomainen käytäntö käyttöjärjestelmän tietoturvan takaamiseksi on tietokoneelle luotujen käyttäjätilien oikeuksien rajoittaminen. Useissa muissa käyttöjärjestelmissä tavallisen käyttäjätilin toimintaa ja oikeuksia on rajoitettu pitkään tietoturvan nimissä, mutta Windows-tuotteiden kanssa tähän on herätty vasta vähän myöhemmin. Tietoturvan kannalta kuitenkin on viisas käytäntö, että käyttäjälle annetaan normaaliin tietokoneen käyttöön vain ne oikeudet joita hän välttämättä tarvitsee. Iltapäivälehtien, sähköpostin ja keskustelupalstojen selaamiseen käyttäjä ei tarvitse oikeuksia asetusten muuttamiselle tai laitteiden ja ohjelmien asennukselle. (Järvinen 2006, 195.)

Pääsääntöisesti Windows-käyttöjärjestelmien erilaiset käyttäjäprofiilit jaetaan järjestelmänvalvojiin (admin) ja peruskäyttäjiin. Pähkinänkuoressa järjestelmänvalvojan oikeudet antavat käyttäjälle valtuudet tehdä muutoksia järjestelmän asetuksiin sekä asentaa uusia päivityksiä, laitteita ja ohjelmia. Normaalissa arkisessa käytössä tällaisia oikeuksia ei kuitenkaan useimmiten tarvita. Peruskäyttäjätili riittää hyvin tavanomaista verkon selailua, viihdekäyttöä ja työasioiden hoitoa varten. Tarpeeton tietokoneen käyttäminen järjestelmänvalvojana on riski, sillä aktiivinen tili jolla voidaan tehdä kaikenlaisia muutoksia koneeseen sekä asentaa uusia ohjelmia, on ihanteellinen kanava rikollisille levittää haitallisia ohjelmiaan. Turvallisinta on käyttää päivittäiseen koneen käyttöön peruskäyttäjän oikeuksin varattua tiliä. Jos ilmenee tarve asentaa, päivittää tai muuttaa jotain, järjestelmä tiedustelee käyttäjältä järjestelmänvalvojan tunnuksia ja salasanaa. Muutoksien tekemiseen oikeutettu käyttäjä tietää nämä tiedot, syöttää ne järjestelmään, tekee muutokset ja tämän jälkeen jatkaa työskentelyä jälleen peruskäyttäjänä. Tietoturvaa lisäävä vaikutus on myös sillä, että kaikkiin asennuksiin ja muutoksiin pääsääntöisesti peruskäyttäjältä vaaditaan järjestelmänvalvojan salasana. Täten käyttäjä ei pääse puolihuolimattomasti klikkailtuaan asentamaan jotain mitä ei pitäisi asentaakaan, sillä kaikki mahdollisesti järjestelmän kannalta kriittiset toimenpiteet tulee vahvistaa vielä kirjoittamalla oikea salasana. (Rousku 2014, 263 – 264.)

6.2 Palomuuri

Palomuuri on laite tai ohjelmisto, jonka tehtävä on estää asiattomien tahojen pääsy verkkoon tai palveluun jota verkko tarjoaa (Hakala 2006, 187). Palomuuri tarkkailee liikennettä koneen ja internetin välillä. Verkon ja tietokoneen välillä liikkuvien datapakettien tekniset tiedot ja palomuurille asetetut säännöt määräävät päästääkö palomuuri liikenteen kulkemaan vai estääkö palomuuri sen. Tämä tuo käyttäjälle suojaa haitallista ja ei-toivottua liikennettä vastaan. Tällaista ei-toivottua haitallista liikennettä ovat mm. haittaohjelmien leviäminen ja hakkerien yritykset murtautua koneelle. Täten palomuurilla on korvaamaton ja tärkeä rooli kodin verkon tietoturvan ylläpitämisessä, eikä palomuurin puuttumista voi korvata. (Järvinen 2012, 189.) Palomuuri ei kuitenkaan suojaa esimerkiksi sähköpostiviruksilta tai muilta haittaohjelmilta, joita käyttäjä lataa (Järvinen 2012, 194).

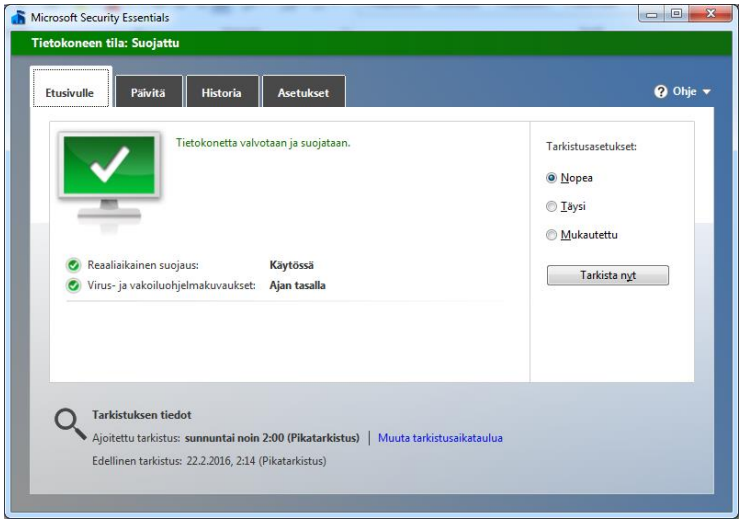
Palomuurit jaetaan yleisesti ohjelmallisiin palomuureihin ja laitepalomuureihin. Ohjelmallinen palomuuri on ohjelma käyttäjän tietokoneella, joka seuraa tietokoneelle tulevaa liikennettä. (Järvinen 2012, 189.) Laitepalomuuri taasen on internetin ja kodin lähiverkon väliin kytketty laite, joka seuraa lähiverkon ja internetin välistä liikennettä. Useimmiten kotikäytössä laitepalomuurin ominaisuudet löytyvät ADSL-modeemista tai WLAN-tukiasemasta. (Järvinen 2012, 190.)

Ohjelmallinen palomuuri lienee kotioloissa yleisempi, sillä se on huomattavasti helpompi tavallisen käyttäjän ottaa käyttöön. Uusimmissa Windows-koneissa tällainen ohjelmallinen palomuuri on asennettu käyttäjälle valmiiksi ja automaattisesti käyttöönotettu. Ohjelmallinen palomuuri pitää käyttäjän tiedotettuna tietokoneen yhteyksistä, ilmoittaen uusista yhteyksistä ja anoen lupia tehdä palomuuriin aukkoja uusille ohjelmille. Tämä on myös samalla ohjelmallisen palomuurin heikkous, sillä joillekin käyttäjille jatkuvat ilmoitukset ja kysymykset yhteyksistä ovat liian teknisiä. Jatkuva outojen kysymysten pommittaminen saattaa johtaa käyttäjän taholta vääriin ratkaisuihin: haitallisen yhteyden hyväksymiseen tai kenties koko palomuuriohjelman kytkemiseen pois päältä. Tavallisessa kotikäytössä paras tietoturvaohjelmisto on pitkälle automatisoitu ja helppo käyttää. Tavallisena tietokoneohjelmana ohjelmallinen palomuuri on tietenkin altis väärinkäytöille. Koneelle esimerkiksi sähköpostin kautta huomaamattomasti hiipinyt haittaohjelma voi sammuttaa palomuurin, altistaen koneen samalla useille muille ulkopuolisille uhille. Tämänkin vuoksi käyttäjätilien oikeuksien rajoittaminen on tärkeää, sillä peruskäyttäjän oikeuksilla palomuurin sammuttaminen ei onnistu. Ohjelmallisen palomuurin ehdottomaksi eduksi voi laskea kyvyn havaita uhkaavia yhteyksiä kotiverkon sisällä. Näin esimerkiksi lasten käyttämistä laitteista tartunnat eivät pääse leviämään saman verkon sisällä kodin tärkeisiin koneisiin. (Järvinen 2006, 110.) Tärkeä ohje ohjelmallisten palomuurien käyttöön on, että ei ole suositeltavaa käyttää useampaa palomuuriohjelmaa samanaikaisesti. Ohjelmallista palomuuria ja laitepalomuuria on jopa suositeltavaa käyttää yhteistyössä, mutta useammat ohjelmalliset palomuurit samassa koneessa sekoittavat toisensa täydellisesti, johtaen ongelmiin. (Järvinen 2012, 190.)

6.3 Virustorjunta

Virustorjunnan vastuualuetta on etsiä ja tuhota haitallisia prosesseja ja tiedostoja. Toimiva virustorjunta pyrkii myös estämään havaittujen tartuntojen leviämisen laajemmalle alueelle. Useimmat virustorjuntaohjelmistot tarjoavat käyttäjälle reaaliaikaista suojaa, jossa ohjelma tarkastelee jatkuvasti tietokonetta mahdollisten uhkien varalta. Osa tartuntojen leviämisen estämistä on uusien kytkettyjen muistilaitteiden, esimerkiksi usb-muistien tarkistaminen.

Kotikäyttöön tarkoitettujen konepakettien yhteydessä mukaan tulee usein valmiiksi asennettu virustorjuntaohjelmisto. Toisinaan kyse on kuitenkin kokeiluohjelmasta, joka vaatii myöhemmin rekisteröintiä ja lisenssimaksun suorittamista jotta ohjelman käyttö voisi jatkua. Maksulliset ohjelmat pitävät sisällään kattavammin erilaisia lisätoimintoja. (Järvinen 2012, 202 – 203.) Realismia lienee kuitenkin se, että tavallinen käyttäjä tarvitsee yksinkertaisen ja helposti käytettävissä olevan tietoturvaohjelmiston, eikä suinkaan kosolti kaikenlaisia lisätoimintoja. Maksulliset virustorjuntaohjelmat päivittyvät nopeammin sekä tunnistavat aiemmin uudentyyppisiä haittaohjelmia (Järvinen 2012, 210). Erot tässä kategoriassa laadukkaiden ilmaisten ja maksullisten ohjelmien välillä ovat pieniä. Ilmaiset virustorjuntaohjelmistot ovat aivan riittäviä kotikoneen suojaamiseen. Hyviä ilmaisia virustorjuntaohjelmia on tarjolla monia, esimerkiksi Microsoftin Security Essentials (kuva 3) tai Avast Free Antivirus.



Kuva 3. Microsoftin tarjoama Security Essentials ohjelmisto on helppokäyttöinen ja ilmainen vaihtoehto kotikoneen turvaksi.

Virustorjuntakaan ei vapauta käyttäjää vastuusta, eikä korvaa oman harkinnan käyttöä. Vaikka virustorjunta ei huomauttaisikaan tiedoston olevan haitallinen, ei se silti tee tiedostosta välttämättä turvallista. Parhaimmatkin ohjelmat ovat erehtyväisiä ja rikolliset pyrkivät kehittelemään jatkuvasti uusia keinoja hämätäkseen tietoturvaohjelmia. Uudenlaisen, uniikin viruksen ilmestyessä alle 10 prosenttia käytetyimmistä ohjelmista tunnistaa tiedoston haitalliseksi (Järvinen

2012, 210). Mahdollista on, että torjuntaohjelmistojen muut suojaukset silti aktivoituvat ja estävät tällaisen tiedoston avaamisen. Jotta virustorjunta voisi toimia tehokkaana suojana uusimpia haittaohjelmia vastaan, se tarvitsee tiedot uusimmista uhista. Tämän vuoksi virustorjunnan ja uusimpien haittaohjelmien kuvauksien päivittäminen on tärkeää ohjelman toimimisen kannalta.

6.4 Langattomat verkot

Langattomien verkkojen yleistyminen on helpottanut elämää huomattavasti. Kotona laitteet voi yhdistää verkkoon missä vain ja matkalla ilmaisen kaikille avoimen verkon löytäminen lienee iloinen yllätys. Harva enää kaipaakaan verkkojohdon avulla nettiin kytkeytymistä, sillä langattomat verkot ovat käyttömukavuudeltaan ylivertainen vaihtoehto. Kehitys kohti langattomuutta on tuonut myös uusia tietoturvariskejä, joista valistuneen tietoyhteiskunnan jäsenen tulisi olla tietoinen. Toisinaan avoimeksi jätettyyn verkkoon liittyminen voi olla suuri tietoturvariski. Oma kotiverkko tulisi osata suojata ja estää ulkopuolisten tahojen pääsy verkkoon. Matkalla ollessa hotellin langattoman yhteyden käyttäminen saattaa maksaa maltaita. Tietoturva on aina tasapainottelua käyttömukavuuden ja maksimaalisen turvallisuuden välillä. Langattomat verkot tarjoavat suurta käyttömukavuutta, mutta samalla käyttäjän tulee tunnistaa siihen liittyvät mahdolliset riskit.

Langatonta verkkoa kutsutaan usein nimellä WLAN (wireless local area network). Jossain yhteyksissä langatonta yhteyttä saatetaan kutsua myös nimellä Wi-Fi (wireless fidelity). Langattomia tietoliikenneyhteyksiä käytetään yleensä kaikenlaisiin sellaisiin yhteyksiin, joissa helppokäyttöisyys ja käyttömukavuus ovat tärkeässä osassa. Näin esimerkiksi kodeissa, kouluissa, kahviloissa ja yleisillä paikoilla tarjotaan usein langattomia yhteyksiä, jotta käyttäjät pääsisivät verkon palveluihin käsiksi vaivattomasti. Langaton liikenne on alttiimpi erilaisille häiriötekijöille ja vakoilulle, joten tärkeät tietojärjestelmät käyttävät lähestulkoon poikkeuksetta kiinteitä yhteyksiä (Andreasson 2013, 73).

WLAN käyttää radiosignaaleja tiedon kuljettamiseen. Tämä poistaa johdon tarpeen, mutta radioliikenne on myös samalla hyvin altis kaikenlaisille häiriötekijöille. WLAN-tukiaseman ja päätelaitteen (tietokoneen, puhelimen tai tabletin) välinen yhteys voi heikentyä huoneistojen rakenteiden takia. Radioliikenne ei hirveän tehokkaasti läpäise kiinteitä esteitä, esimerkiksi seiniä. Myös muut samalla taajuusalueella toimivat WLAN-verkot ja tukiasemat saattavat aiheuttaa signaalin häiriötä. Myös joka kodin kodinkoneet saattavat aiheuttaa häiriötä signaalissa, sillä esimerkiksi mikroaaltouunien on huomattu häiritsevän WLAN-verkkojen toimintaa. (Hakala 2006, 293.) Pahansuopa naapuri voi myös yrittää estää langattoman verkon toimintaa tehokkaiden lähettimien ja suunta-antennien avulla. WLAN-verkkojen eduksi usein lasketaan mahdollisten laitteiden käyttö missä vain signaalin kuuluvuusalueella, sillä käyttäjät eivät ole sidottuja johtojen vuoksi. Vaikka hyvä kuuluvuus koko huoneistossa onkin iloinen asia, saattaa signaali myös ulottua rakennuksen ulkopuolelle. Näin

WLAN-tukiasema saattaa olla tavoitettavissa naapurinkin toimesta. (Andreasson 2013, 73.)

Langattoman verkon turvalliseen käyttöön kuuluu olennaisena osana tietoliikenteen salaaminen asiattomilta tahoilta, sillä sopivan apuohjelman avulla urkkija voi nähdä ison osan tukiaseman ja päätelaitteiden välisestä liikenteestä. Tästä huolimatta toisinaan varsinkin kotikäyttöön asennetuissa langattomissa verkoissa verkon salauksen käyttöönotto on laiminlyöty. SSL-salausta käyttävä liikenne on täten salattua (esimerkiksi pankissa asiointi), mutta muu liikenne liikkuu tietokoneen ja tukiaseman välillä täysin salaamattomana. Hyvä käytäntö on ottaa käyttöön WPA2 tietoturvastandardi. Tämä mahdollistaa käyttäjien edistyneemmän tunnistamisen ja tietoliikenteen salauksen. Tietoliikenteen salaukseen WPA2:n kanssa suositellaan AES-salausta. (Rousku 2014, 212.)

Miten on mahdollista tehdä kodin langattomasta verkosta turvallinen? Onko se edes mitenkään mahdollista, kun kaikenlaisia haasteita tuntuu olevan lukuisia? Kodin langattomasta verkosta on mahdollista tehdä riittävän turvallinen muutamilla muutoksilla. Tietoturva on ainaista kamppailua käyttömukavuuden ja täydellisen turvallisuuden välillä. Langattomista verkoista tuskin saadaan koskaan täysin turvallisia, mutta asiallisilla toimenpiteillä kodin verkon voi saada riittävän turvalliseksi arkiseen käyttöön.

WLAN-tukiasemaa ensimmäistä kertaa määrittäessä on viisainta vaihtaa laitteen hallintatunnuksen salasana. Tavanomaisesti näiden laitteiden hallintatunnukset ja oletussalasanat löytyvät pikaisella tiedonhaulla internetistä, joten oletussalasana ei sinällään estä juuri ketään pääsemästä käsiksi laitteeseen. Tämän vuoksi salasanan vaihtaminen on tärkeää. Samalla kannattaa myös estää tukiaseman asetusten muokkaaminen netin välityksellä, sekä estää laitteen hallinta langattomasti. Näin tukiaseman asetusten muuttamiseksi käyttäjän täytyy olla tietokoneineen johdon kautta yhteydessä laitteeseen. Tämä estää ison osan väärinkäytöksistä. Tukiaseman asetuksista voi usein laskea tämän lähetystehon voimakkuutta. Pienissä kerrostaloasunnoissa pienempikin laitteen lähetysteho riittää helposti kattamaan koko asuintilan ja täydellä teholla signaali leviää ulkopuolistenkin tavoiteltavaksi. Lähetystehoa laskemalla saadaan kavennettua mahdollisten ulkopuolisten käyttäjien pääsyä käsiksi verkkoon. Olennaista on asettaa omalle langattomalle verkolle vahva salasana, sekä antaa verkolle nimi joka erottaa sen muista alueen verkoista. SSID (service set identifier) tarkoittaa langattoman verkon nimeä joka erottaa sen muista verkoista. Halutessaan käyttäjä voi piilottaa verkon SSID:n, jolloin verkko ei oletusarvoisesti näy tarjolla olevia verkkoja selatessa. Täten verkkoon pääsee liittymään tietämällä oikean SSID-nimen, sekä verkon salasanan. Langattomaan verkkoon liittyviä laitteita voi myös rajoittaa laitekohtaisten MAC-osoitteiden avulla. Jokaisella laitteella on oma MAC-osoitteensa, joten tukiasema voi suodattaa laitteita sen mukaan onko tämä osoite hyväksyttyjen osoitteiden listalla. SSID:n piilottaminen ja MAC-osoitteiden mukaan tapahtuva rajoitus ovat kuitenkin keinoja, jotka ovat sopivien apuohjelmien avulla helposti kierrettävissä. Täten näitä ei voi varsinaisesti käyttää ainoina pääsynvalvonnan keinoina, sillä motivoitunut yksilö

kiertää nämä esteet. Nämä ovat kuitenkin käyttökelpoisia keinoja verkon kulunvalvontaan. (Rousku 2014, 210 – 211.)

Useissa WLAN-tukiasemissa on käytössä WPS-tekniikka, joka on suunniteltu helpottamaan laitteiden liittämistä langattomaan verkkoon. Tämä tekniikka on kuitenkin sittemmin todettu tietoturvariskiksi ja sen käyttöä ei enää suositella. Viisainta onkin poistaa WPS-tekniikka käytöstä kodin tukiasemasta, mikäli mahdollista. (Viestintävirasto 2012.)

Kuten tässä työssä on jo aiemmin esitelty, päivitykset ovat ehdottoman tärkeitä, jotta laitteet ja ohjelmat voisivat toimia oikein. Päivityksiä julkaistaan, koska tuotteessa on havaittu ongelmia, virheitä tai tietoturva-aukkoja jotka vaativat korjausta. Tuotteiden valmistajat pyrkivät tuomaan markkinoille täydellisen tuotteen, mutta usein vasta ohjelman laaja käyttöönotto paljastaa todelliset kehityskohteet. Päivitysten julkaiseminen on tietysti valmistajalle harmillista, sillä tuote vaatikin korjausta eikä ollutkaan niin valmis kuin olisi voinut luulla. Samalla päivitysten asentaminen on myös käyttäjille harmillista, sillä se vaatii ylimääräistä työtä. Tärkeiden ohjelmien ja laitteiden toimivuus on kuitenkin niin tärkeää, että mahdolliset ongelmat ja tietoturva-aukot on tärkeää saada niistä korjattua. Vaikka päivitysten asentaminen tuntuisi turhalta vaivalta, ohjelmien päivittäminen on kuitenkin ensiarvoisen tärkeää, jotta kaikki toimisi halutulla tavalla. Mikään taho ei julkaise päivityksiä huvin vuoksi tai sen työllistävän vaikutuksen takia, vaan mahdollisille korjauksille on usein hyvin painava syy. Lähiverkon toimimisen kannalta olisi täten tärkeää tarkistaa tukiaseman päivitysten saatavuus. Mahdollista on, että tukiaseman laitevalmistaja on julkaissut markkinoille firmware-päivityksen. Firmwarella tarkoitetaan laitteen ohjelmistoa, joka vastaa yksinkertaistetusti laitteen toiminnasta. Tämän päivityksen lataaminen ja asentaminen takaa osaltaan laitteen toimimisen suunnitellusti. Päivitys saattaa myös sisältää tärkeitä tietoturvapäivityksiä, jotka tukkivat laitteen tunnetut tietoturva-aukot. (Rousku 2014, 210.)

Kodin omaan verkkoon, jota itse hallinnoi ohjeiden ja säännösten mukaisesti, voi suhteellisen turvallisin mielin liittyä päivästä toiseen. Kodin ulkopuolella ja varsinkin matkoilla kohtaa lukuisia langattomia verkkoja, joiden turvallisuudesta ja näitä hallinnoivan tahon aikeista ei voi olla täysin varma. Kuka tahansa voi pystyttää langattoman verkon ja tarjota sen palveluita muille henkilöille. Jotkut langattomat verkot saattavat olla huijausverkkoja tai niiden käyttöehdot saattavat lähennellä enemmänkin käyttäjien riistoa ja sumuttamista kuin oikeaa rehellistä palvelua. Tietoturvallisin ratkaisu olisi käyttää vain esimerkiksi hotellin tarjoamaa langallista yhteyttä, jos sellainen on tarjolla (Järvinen 2012, 273). Usein tällaista vaihtoehtoa ei kuitenkaan ole. Voi olla hyvin haasteellista tunnistaa, mitkä julkisista verkoista ovat turvallisia ja mitkä eivät. On olemassa muutamia seikkoja, jotka kannattaa pitää mielessä kun etsii luotettavaa langatonta verkkoa kodin ulkopuolelta.

Turistikohteessa kaikelle kansalle avoimeen verkkoon törmääminen voi tuntua miellyttävältä yllätykseltä, mutta avoimeen verkkoon liittymiseen saattaa sisäl-

tyä muutamia merkittäviä riskejä. Ensinnäkin käyttäjälle saattaa olla täysi mysteeri, mikä taho verkon ylläpidosta vastaa ja mitkä tämän tahon motiivit ovat ilmaisen palvelun tarjoamiselle. Kyseessä saattaa jopa olla ns. hunajapurkki, houkuttava ansa johon pyritään huijaamaan käyttäjiä (Järvinen 2012, 276). Verkosta vastaava taho saattaa seurata käyttäjien toimintaa, valvoa salaamatonta liikennettä ja pyrkiä poimimaan käyttäjien tietoja. Suositun yleisen verkon jokaisen käyttäjän rehellisyydestä ei voi päästä takuuseen. Joku verkon käyttäjistä voi myös kuunnella verkon kaikkea liikennettä ja pyrkiä poimimaan muiden käyttäjien arkaluontoisia tietoja (Järvinen 2012, 275). Avoimessa langattomassa verkossa vain HTTPS-salatut yhteydet ovat turvallisia, kaiken muun liikenteen ollessa enemmän tai vähemmän ulkopuolisten tahojen nähtävillä. (Järvinen 2012, 276.) Tietoturvan kannalta parempi ratkaisu on asioida käyttäen esimerkiksi hotellin verkkoa, sillä yleensä nämä ovat suojattu käyttäjätunnuksin ja salasanoin. Näin ulkopuoliset tahot pysyvät hieman paremmin poissa ja verkon käyttäjien suhteen on olemassa jonkinlaista kulunvalvontaa. Usein kuitenkin, varsinkin ulkomailla, hotellien verkkojen käytöstä veloitetaan melko röyhkeitäkin summia. Toisaalta taas nämä maksulliset verkot ovat usein salattuja ja siten turvallisempia kuin täysin avoimet ja suojaamattomat verkot. (Järvinen 2012, 274.) Maksullisia WLAN-verkkoja käyttäessä tulisi olla erityisen tarkka siitä, mitä tietojaan antaa muiden käytettäväksi. Turvalliselta ja luotettavalta vaikuttava palvelu saattaa tiedustella vähän turhankin innokkaasti käyttäjän luottokorttitietoja ja muita yksityisiä tietoja. Tiedot saatuaan palvelu saattaa päästää käyttäjän käsiksi verkkoon, mutta samalla palvelun haltija on saanut käsiinsä arkaluontoisia tietoja joita ei tulisi luovuttaa ulkopuolisten käsiin. Arkaluontoisten tietojen, esimerkiksi luottokorttitietojen, luovuttamista tulisi välttää. Turvallisinta lienee käyttää vain maassa rehellisiksi toimijoiksi tunnettujen tahojen maksullisia WLAN-palveluita ja lukea tarkkaan palvelun käyttöehdot. (Rousku 2014, 215.)

6.5 Tärkeiden tiedostojen turvaaminen

Tiedon siirtyminen verkkoon ja sähköiseen muotoon on luonut ihmiskunnalle uusia haasteita. Tärkeät dokumentit, työt ja asiakirjat ovat täysin tietotekniikan ratkaisujen ja niiden toimisen armoilla. Internetin syövereihin tallennettu tieto säilyy kyllä pitkään, mutta henkilökohtaisille tallennuslaitteille varastoitu tieto saattaa hävitä ikuisiksi ajoiksi katastrofin myötä. Sosiaaliseen mediaan vahingossa tallennettu kiusallinen kuva jää elämään internetiin omaa elämäänsä, vastoin käyttäjän tahtoa, mutta rakkaat yksityiset valokuvat saattavat laiterikon myötä hävitä tavoittamattomiin. Sähköisesti tallennetut dokumentit eivät säily ikuisesti, sillä tietotekniikan tallennuslaitteita ei ole edes suunniteltu toimimaan loputtomasti. Tästä huolimatta useimmat toimivat tärkeiden, korvaamattomien tiedostojensa kanssa hyvin huolimattomasti. Korvaamattomia työprojekteja ja tärkeitä dokumentteja säilötään tietokoneella toivoen vain, että katastrofi ei tapahtuisi. Toisinaan kriisitilanteessa tiedostot saattavat olla pelastettavissa, löydettävissä sähköpostista tai vaikkapa työpaikan koneelta, mutta tärkeiden tietojen tallennukseen liittyviin riskeihin havahdutaan vasta ongelman ilmaannut-

tua. Vastuullinen tietoyhteiskunnan jäsen turvaa tärkeät tietonsa ennen mahdollisen katastrofin syntyä, sillä hyvin harva meistä on kykeneväinen ennustamaan tulevaisuutta. Laiterikko, laitteen katoaminen, varkaus tai tulipalo tulevat usein ihmisille täytenä yllätyksenä, eikä kukaan tällaisia ikäviä asioita osaa ennustaa etukäteen tapahtuvaksi. Täten näihin on tärkeää varautua etukäteen. Ongelmiin voi ja on syytä varautua etukäteen. Useimmat keinot ainakin vähän vähentävät tietojen häviämisestä johtuvaa tuskaa, vaikka eivät täysin kaikkia mahdollisia katastrofiskenaarioita eliminoisikaan.

Tietojen häviämistä voi pyrkiä estämään erilaisilla tietoteknisillä laiteratkaisuilla. Vastuullinen tietokoneen omistaja pyrkii vaihtamaan koneen tallennusmediat ajoissa uusiin, ennen niiden hajoamista. Tärkeä osa tietojen säilyttämistä on varmuuskopiointi. Näin tiedot ovat turvassa jollain toisella tallennuslaitteella tai -palvelulla, vaikka alkuperäiseen tiedostoon ei enää pääsisikään käsiksi. Tiedostojen varmuuskopioita tehdessä on myös hyvä huomioida varmuuskopion sijainti. Mikäli kannettavalta tietokoneelta varmuuskopioitu tiedosto löytyy ainoastaan muistitikulta, joka on samassa laukussa kannettavan kanssa, ei varmuuskopiosta ole hirveästi hyötyä jos kannettava tietokone laukkuineen varastetaan. Tulipalon tapahtuessa ulkoisella kiintolevyllä sijaitsevat varmuuskopiot saattavat todennäköisesti tuhoutua siinä missä itse tietokonekin. Tietenkin todennäköisyys näille tapahtumille on pieni, mutta mikäli kyseessä on todella kallisarvoinen työ tai dokumentti kannattaa vahvasti harkita sen säilömistä jonnekin toiseen tilaan itse alkuperäisen tiedon kanssa. Mikäli säilyttää esimerkiksi kannettavalla tietokoneella jotain erityisen arkaluontoista ja yksityistä tietoa, kannattaa myös harkita tiedostojen salaamista. Täten ulkopuolinen taho, esimerkiksi tietokonevaras, ei pääse näkemään tietoja tietämättä oikeaa avainta.

Tietokoneen data, tiedostot ja ohjelmat tallennetaan kiintolevyille. Arkikielessä kiintolevyistä puhutaan joskus kovalevyinä. Kiintolevy on olennainen osa tietokoneen kokonaisuutta, sillä se mahdollistaa levylle asennetun käyttöjärjestelmän nopean toimimisen. Kiintolevylle kirjoittuvat kaikki käyttäjän tallentamat tiedostot, lomakuvat ja työprojektit, joten sen toimiminen on ensiarvoisen tärkeää tietojen säilymisen kannalta. Kiintolevyt ovat kuitenkin kuluvia osia, jotka ennemmin tai myöhemmin hajoavat. Tämä asettaa käyttäjät mielenkiintoiseen tilanteeseen, sillä liian usein levyn vaihtaminen tuntuisi tuhlaukselta, mutta samalla levyn hajoamiseen asti odottaminen voi johtaa tietojen katoamiseen.

Kiintolevymarkkinoiden kehitys on johtanut mielenkiintoiseen tilanteeseen käyttäjien kannalta. Tallennuskapasiteetti on kasvanut hurjasti ja levyt ovat varsin huokeita. Kuluttajan kannalta tilanne on riemukas, mutta samalla isot kiintolevyt eivät juuri pakota käyttäjiä arkistoimaan tiedostojaan ja valikoimaan mikä on tärkeää ja mikä ei. Mahdollisen laiterikon tapahtuessa myös paljon tietoja katoaa. Käyttäjille levyn tallennuskapasiteetin määrä, kilpailukykyinen hinta ja nopeus ovat osoittautuneet tärkeämmäksi kuin vankka toimintavarmuus. Tämä on johtanut levyjen vähentyneeseen toimintavarmuuteen. Nykyisten kiintolevyjen voi odottaa toimivan täysin varmasti vain niiden muutaman vuoden takuuajan verran. Kolhut, lämpö ja yleinen käyttö kuluttavat levyä ja

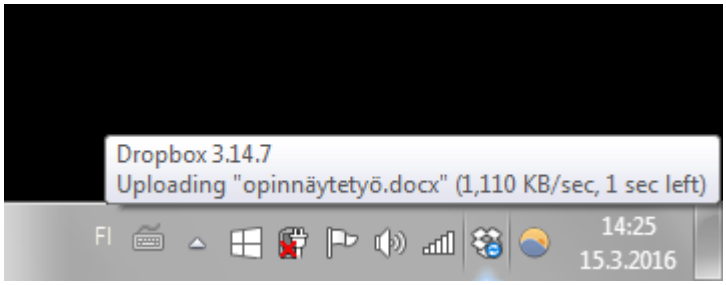
täten kaikki levyt hajoavat aikanaan. Näin ollen kiintolevyä voisi ennemminkin luonnehtia tilapäiseksi tiedon säilytyspaikaksi. (Järvinen 2006, 324.)

MTBF-arvo kuvastaa kiintolevyn keskimääräistä toiminta-aikaa ennen hajoamista. MTBF on lyhenne sanoista Mean Time Between Failures. Nämä lukemat usein mitataan laboratorio-olosuhteissa, joissa levy ei juuri kohtaa kolhuja, lämpöä tai varsinaisesti työskentelystä johtuvaa kuormitustakaan. Täten MTBF-arvo on usein varsin epärealistinen mittari levyn todellisesta eliniästä. Parempi mittari levyn kestävyydestä on service life, joka ilmoitetaan vuosissa ja edustaa tuotteen odotettua elinikää. Useimmiten tuotteen valmistajat ounastelevat tuotteen kestävän kolmesta viiteen vuotta. Hyvällä lykyllä tuote voi kestää kauemminkin, mutta laiterikon riski on huomattavasti kohonnut tämän jälkeen. Täten hyvä nyrkkisääntö olisi vaihtaa kiintolevyt ainakin viiden vuoden välein tai ainakin varautua mahdolliseen vaurioitumiseen varmuuskopioimalla tärkeät tiedostot. (Järvinen 2006, 324 – 325.)

Tärkeiden tietojen varmistamiseen voi käyttää esimerkiksi USB-liitäntään kytkettävää ulkoista kiintolevyä. Tällainen liikuteltava laite tarjoaa tallennustilaa vaikka perheen kaikkien tietokoneiden tärkeille tiedoille, sillä ulkoista kiintolevyä voi kuljettaa mukanaan laitteesta toiseen. Toisinaan ihmiset saattavat käyttää tärkeiden tiedostojen siirtämiseen ja säilyttämiseen myös USB-muistitikkuja, jotka ovat pienikokoisia ja täten helppoja siirtää koneesta toiseen. USB-liitäntään kytkettävät laitteet tarjoavat käyttökelpoisen ja helpon tavan säilöä ja liikutella tärkeitä tiedostoja. Kuten tavanomaiset kiintolevyt, myös nämä laitteet voitaisiin luokitella tilapäisesti toimiviksi tiedon tallennuspaikoiksi. (Järvinen 2006, 335.) Kattavinkin varmuuskopiointi on turhaa, mikäli varmistetun tiedon säilytyspaikan sijoittaa suoraa alkuperäisen tiedonlähteen välittömään läheisyyteen. Muistitikulle varmistetuista työprojekteista ei ole paljon iloa, jos muistitikku sijaitsee varkaan mukaan lähteneessä läppärilaukussa tietokoneen kanssa.

Tietotekniikan kehittyminen ja tiedon siirtyminen verkkoon on tuonut myös tietojen varmuuskopiointiin uusia vaihtoehtoja. Pilvipalvelujen kehitys on mahdollistanut tietojen käsittelyn lähestulkoon laitteelta kuin laitteelta, mistä vain, kunhan vain Internet-yhteys on saatavilla. Pilvipalvelu on yleisnimitys ohjelmille ja palveluille, jotka ovat siirtyneet verkkoon paikallisen kotikoneella toimimisen sijaan. Tämä vapauttaa käyttäjän työstämään tiedostojaan missä vain, sillä esimerkiksi työprojekti on saatavilla internetin välityksellä niin työkoneelta, tabletilta, puhelimelta kuin myös kotikoneelta. Käyttäjä tarvitsee vain nettiyhteyden. Pilvipalvelut tarjoavat täten myös tietojen säilytystilaa verkossa. Näin säilyttämisen arvoiset tiedostot voikin vain ladata verkossa sijaitsevaan palveluun. Samalla myös tiedostot sijaitsevat oman kodin, usein jopa oman kotimaan ulkopuolella, joten tulipalon, tulvan, lumivyöryn tai varkauden sattuessa tiedot ovat silti saatavilla verkossa. Esimerkkejä tällaisista pilvipalveluista ovat Microsoftin tarjoama Onedrive-palvelu, Googlen Google Drive sekä Dropbox (kuva 4). Pilvipalvelut toki kaikessa helppokäyttöisyydessään aiheuttavat myös pulmia tietoturvan osalta. Palvelun ollessa ulkopuolisen tahon päätösvallan alla, voi palvelu teoriassa lopettaa toimintansa koska vain kadottaen

samalla käyttäjien kaikki tiedot. Kun kyse on ulkopuolisen tahon omistamasta palvelusta, todella salaisten ja yksityisten tietojen säilyttämiseen kannattaa suhtautua varauksella. Yrityssalaisuuksien lataaminen pilveen saattaa jopa yrityksen tietoturvapolitiikassa olla kielletty. Pilvipalvelut vaativat myös Internet-yhteyden. Tärkeisiin tiedostoihin ei siis pääse käsiksi, mikäli yrityspalaveri pidetään metsästysmajassa keskellä suomalaista korpimetsää puhelin- ja verkkoyhteyksien tavoittamattomissa. (Rousku 2014, 186 – 191.)



Kuva 4. Dropbox lataa tärkeää tiedostoa pilveen turvaan luonnonkatastrofeilta, tulipalolta, kiintolevyn hajoamiselta ja tietokonerosvoilta.

Joskus on kuitenkin syytä varautua pahimpaan. Salakirjoitus on turvallinen tapa estää ulkopuolisia henkilöitä näkemästä mitä tiedostot tai massamuistit pitävät sisällään. Salakirjoitetun levyaseman tai tiedoston onnistuneeseen lukemiseen tarvitaan oikea salausavain. Vaikka tämä kuulostaa mainiolta asialta ja idioottivarmalta keinolta kohentaa tietoturvaa, sisältää salakirjoitus kuitenkin muutamia ongelmia. Salauksen perustuessa täysin oikean salasanan tietämiseen, vaatii onnistunut tiedostojen salaus hyvien salasanakäytäntöjen noudattamista. Valitun salasanan muistaminen on ensiarvoisen tärkeää. Lienee todennäköisempi vaihtoehto, että käyttäjä unohtaa valitsemansa salasanan kuin että tiedosto joutuisi varkaan kynsiin. Levyaseman hajotessa yllättäen salakirjoitus tekee tiedostojen pelastamisesta mahdotonta. Salausta käytettäessä varmuuskopioinnin merkitys korostuu. Salaus on kuitenkin käyttökelpoinen keino suojata tiedostoja, mikäli on huolissaan yksityisten tietojen turvallisuudesta. Koko levyn salaamiseen voi käyttää esimerkiksi Microsoftin BitLocker-toimintoa tai TrueCrypt-ohjelmaa. Toisinaan on käytännöllisempää ja helpompaa salata vain yksi tiedosto, kun kyse on esimerkiksi salaisen työtiedoston lähettämisestä työkaverille. Tällaisia tapauksia varten toimisto-ohjelmistoissa, kuten esimerkiksi Microsoftin Officessa sekä ilmaisissa Openofficessa ja Libreofficessa, on olemassa mahdollisuus salata yksittäisiä tiedostoja. Uusimmissa versioissa salaus perustuu AES-algoritmille, joka on käytännössä katsoen hyvin turvallinen. (Järvinen 2012, 225 – 226.)

Tiedostojen säilyttäminen ja suojeleminen kaikenlaisilta uhilta nähdään usein yhtenä tärkeimmistä tietoturvan osa-alueista. Vähintään yhtä tärkeää on tiedon tuhoaminen, sitten kun sen aika on. Tiedostojen oikeaoppinen poistaminen varmistaa sen, että tärkeät tiedot eivät päädy ulkopuolisten tahojen haltuun. Usein tietojen asianmukainen tuhoaminen tehdään huolimattomasti tai jopa laiminlyödään täysin. Isojen organisaatioiden ja valtiollisten toimijoiden arkaluontoisia tietoja on joutunut ulkopuolisten tahojen haltuun, kun esimerkiksi vanhoja

kiintolevyjä on myyty tai annettu eteenpäin poistamatta niiden tietoja. Tavanomaisenkin käyttäjän on syytä laitteista luopuessa tai niitä myydessä poistaa laitteelle tallennetut tiedot oikeaoppisesti. Yleinen käsitys on, että levyn formatointi, eli alustaminen, riittää tietojen poistamiseen levyltä. Tämä ei yksinkertaisesti pidä laisinkaan paikkansa. Alustaminen ainoastaan nollaa levyllä sijaitsevien tiedostojen sijainnista kertovan kirjanpidon. Tieto sijaitsee yhä levyllä ja tiedostot ovat vielä varsin helposti palautettavissa. Tiedostot ovat ikään kuin piilossa, eivätkä suinkaan tuhottu. Mikäli kyseessä on tärkeä tiedosto jonka ei halua joutuvan vääriin käsiin, levyn alustaminen ei riitä. Ei paperille tulostetun yksityisen tiedon hävittämiseksikään riitä paperin piilottaminen, vaan paperi pitää tuhota esimerkiksi silppurilla. Tiedostojen tuhoamiseksi vanhan tiedon päälle tulee kirjoittaa jotain uutta. Näin vanha tieto ei enää ole luettavissa levyltä. Tietojen poistamiseen on paras käyttää jotain levyjen pyyhkimiseen soveltuvaa apuohjelmaa, kuten esimerkiksi Darik's Boot And Nuke tai Eraser. Tällaiset ohjelmat ovat käteviä, mikäli haluaa ottaa kiintolevyn uudelleen käyttöön, mutta poistaa samalla siltä kaikki entiset tiedot. Jos kiintolevylle ei enää ole mitään käyttöä ja vanha levy on lentämässä kaatopaikalle muiden romujen mukana, on tiedostojen tuhoaminen helpompaa. Tässä tapauksessa hyvä käytäntö on fyysisesti tuhota laite. Kiintolevyn voi tuhota varsin helposti vasaralla takoen, varmistaen näin laitteen käyttökelvottomuuden. (Järvinen 2006, 252 – 255.)

7 SOSIAALINEN MEDIA

Sosiaalisesta mediasta on räjähdysmäisesti kasvanut yksi merkittävimmistä ilmiöistä. Sosiaalisen median kanavia hyödyntävät niin yritykset, organisaatiot kuin yksityishenkilötkin. Käsitteenä sosiaalinen media, tai some, kuten jotkut leikkisästi tätä kutsuvat, on varsin laaja. Yleisesti ottaen siihen luetaan kaikki internetin palvelut, joissa käyttäjät jakavat tuottamaansa sisältöä vuorovaikutuksessa muiden henkilöiden kanssa. Tavanomaisesti sosiaaliseksi mediaksi luetaan isot palvelut kuten Facebook, Twitter tai Youtube, mutta myös kaikenlaiset blogit, wikit ja muut yhteisölliset verkkopalvelut kuuluvat tämän termin alle. (Andreasson 2013, 151.)

Sosiaalisen median räjähdysmäinen kasvu on avannut ihmisille lukuisia ennennäkemättömiä mahdollisuuksia ja hyötyjä, mutta myös samalla tarjoaa uusia haasteita tietoturvan ja tietosuojan saralla. Sosiaalinen media houkuttelee kaikenlaisia käyttäjiä vauvasta vaariin. Täten joukkoon mahtuu myös suuri osa henkilöitä, jotka eivät välttämättä ole järin valistuneita tietotekniikkaan liittyvissä asioissa. Sosiaalinen media on avannut haittaohjelmille, pahantekijöille ja rikollisille uuden väylän päästä lähelle merkittävää hyväuskoisten ja varomattomien yksilöiden joukkoa. Nettiin on myös valitettavan helppo jättää jälkensä kirjoittamalla tai tekemällä asioita, joita myöhemmin saattaa katua. Erehdyksessä Facebookiin ladattu kuva tai vuosia sitten tehty harkitsematon kommentti saattaa tulla esiin uudelleen ja uudelleen kiusallisissa yhteyksissä. Vastuu tehdyistä kommenteista tai päivityksistä on aina käyttäjällä ja verkossa pätevät samat hyvän käytöksen normit kuin normaalissakin kanssakäymisessä. Valitettavan usein kuitenkin sosiaalisessa mediassa aikuisetkin ihmiset kirjoittavat asioita joiden seurauksia he eivät oikein tunnu käsittävän. Vaitiolovelvollisuus on voimassa myös verkossa ja kunnianloukkauksesta voi saada syytteen verkkokirjoitusten perusteella (Andreasson 2013, 153). Suurilla organisaatioilla on tätä nykyä käytössä jonkinlaiset sosiaalisen median käyttöä ohjaavat ohjeet, jotka sanelevat käyttäjille millaista käytöstä verkon palveluissa työntekijöiltä odotetaan ja mitä esimerkiksi työasioista on soveliasta kertoa. Sosiaalinen media on hämärtänyt hieman yrityksen työntekijänä ja yksityishenkilönä toimimisen rajaa, sillä usein henkilöt ilmoittavat profiileissaan työpaikkansa ja tittelinsä. Sopimaton käytös ja riidanhaastaminen, vaikkapa uutisartikkelien kommentointipalstalla, jonkin yrityksen edustajana saattaa lyödä vähemmän halutun leiman myös yrityksen imagoon, vaikka kommentteja esitettäisiin vapaa-ajalla yksityishenkilönä. Parhaimmillaan sosiaalinen media yhdistää ihmisiä, luo uusia mahdollisuuksia ja helpottaa kanssakäyntiä. Samalla uudet ilmiöt tuovat kuitenkin mukanaan uudet riskit, haasteet ja ongelmat, joihin joutuu varautumaan.

Pahantekijät ja rikolliset pyrkivät olemaan ihmisten keskellä kepulikonsteineen ja huijauksineen. Suuren yleisön massiivinen ryntäys internetiin ja sosiaaliseen mediaan on ollut täten myös jättipotti kaikenlaisille konnille, sillä sosiaalinen media on tuonut käsittämättömän määrän uusia uhreja aivan heidän ympärilleen. Haittaohjelmien, huijauksien ja arkaluontoisten tietojen urkinnalle sosiaalinen media tarjoaa mitä oivallisimman alustan. Kaverien jakamat pelit, visailut

ja muut linkit saattavat olla haittaohjelmia, mutta käyttäjät harvemmin epäilevät näitä koska luottavat ystäviinsä. Tietoturvavalistus on tehnyt käyttäjistä varovaisia ja epäluuloisia sähköpostin liitetiedostoja kohtaan, mutta sosiaalisen median kautta leviävät haittaohjelmat ovat usein käyttäjille uusi ja yllättävä ilmiö. Esimerkiksi Facebookin sisällä leviävissä haittaohjelmissa käyttäjä usein huiputetaan antamaan haittaohjelmalle riittävät oikeudet, jonka jälkeen haittaohjelma levittää itseään entisestään kirjoittamalla houkuttelevia ilmoituksia käyttäjän nimissä ympäri palvelua. Varomattomat käyttäjät klikkailevat ilmoituksissa olevia linkkejä, saastuttaen samalla omankin tilinsä. Näin haittaohjelma leviää kulovalkean tavoin. Tartunnan jälkeen haittaohjelma pyrkii kenties vakoilemaan käyttäjien tietoja ja sähköpostiosoitteita. Rikollisille sosiaalinen media on suoranainen kultakaivos, sillä yksittäinen huijausviesti saattaa kerätä vuorokauden aikana jopa 250 000 klikkausta. (Andreasson 2013, 166.)

Sosiaalinen media perustuu tietojen jakamiselle, verkostoitumiselle ja sisällön tuottamiselle. Tämä tekee sosiaalisesta mediasta niin suositun ja kiinnostavan, mutta samalla myös johtaa väistämättä muutamiin haasteisiin. Toisinaan blogeissa tai muissa palveluissa jaetaan hyvinkin henkilökohtaisia tietoja ajattelematta sen kummemmin niiden seurauksia. Usein käyttäjät ajattelevat tietojen päätyvän vain lähimpien ystävysten tai tuttavien luettavaksi, mutta hyvin usein samat tiedot ovat kenen tahansa nähtävissä. Lomamatkalle lähtevää kehoitetaan esimerkiksi sopimaan naapurin kanssa postilaatikon tyhjennyksestä, jotta rosvot eivät saisi vihiä talon olevan tyhjillään. Samalla kuitenkin tulevaa lomamatkaa on saatettu mainostaa henkilökohtaisessa blogissa tai muussa sosiaalisen median profiilissa jo kuukausia etukäteen. Itse lomamatkahan ei ole onnistunut ilman tuhansia selfieitä ja päivityksiä sosiaaliseen mediaan keskeltä turistirysien vilinää. Tämän päivän nokkela rosvo istuukin tietokoneensa ääressä seuraamassa ihmisten varomatonta raportointia menemisistä ja tulemisistaan, eikä suinkaan taivalla pakkasessa, tuiskussa ja tuulessa postilaatikolta toiselle. Monet ohjelmat ja palvelut jakavat käyttäjistään kaikenlaisia tietoja, joita tarkemmin pohdittuaan ei välttämättä haluaisikaan tulla antaneeksi kaiken kansan nähtäville. Esimerkiksi monet kuvat pitävät sisällään tarkat kuvauspaikan koordinaatit, joiden avulla voi päätellä missä kuva on tarkalleen ottaen otettu. Urheilusovellukset ilmoittavat usein tarkat tiedot käytetystä reitistä ja ajankohdasta. Jokainen nyt voi omalla tahollaan pohtia haluaisiko illan hämärässä tehtävän vakiojuoksulenkkinsä reitin ja ajankohdan jokaisen sosiaalista mediaa käyttävän hiipparin tietoon. (Andreasson 2013, 159 – 160.)

Sosiaalinen media on myös antanut kaikille uuden väylän julkaista syvimpiä tuntojaan ja kannanottojaan melko julkisella foorumilla. Jokaisella on nykyään ääni joka pitää saada kuulluksi. Tuohtuneessa mielentilassa saattaa tuntua hyvältä kun voi ruotia elämässä kohdattuja vaikeuksia sosiaalisessa mediassa. Pomon tai työkavereiden kovasanainen kritisointi omalla seinällä saattaa helpottaa pahaa oloa, mutta johtanee lisävaikeuksiin kun tieto työntekijän kannanotosta kiirii pomon korviin. Useinhan näissä tapauksissa hetken huumassa unohdetaan, että Facebookissa tuli lisättyä pomo kaveriksi taannoin ja verkkoon toimitettu avautuminen pamahtaa suoraan pomon luettavaksi. Vahingot ja tahattomat paljastukset jäävät elämään internetiin. Jotkut ovat perustaneet

jopa verkkosivuja joille kaikenlaisia kiusallisia sosiaalisessa mediassa tapahtuvia kömmähdyksiä dokumentoidaan. Riemukkaan lomakuvan sijaan profiiliin saattaa väärän klikkauksen myötä vahingossa latautua jonkinlainen yksityinen kuva jota ei välttämättä kehtaisikaan näyttää isoäidilleen. Internet ei anna armoa ja usein nolot kuvat tai tiedot ovat jo ehtineet tallentua ulkopuolisten toimesta, vaikka asianomainen ne jossain vaiheessa ehtisikin poistaa.

Sosiaalinen media ja tietosuoja ovat usein ristiriidassa. Tietosuoja pyrkii suojaamaan käyttäjien tietoja, kun taas sosiaalisen median viehätys on nimenomaan tietojen ja sisällön jakamisessa muiden nähtäväksi. Sosiaalinen media on ikään kuin jättimäinen tietokanta ihmisten tiedoista, osoitteista, suhteista, sijainnista ja keskinäisestä viestinnästä. Esimerkiksi Facebookia on tämän vuoksi luonnehdittu tyrmistyttäväksi ihmisten vakoilukoneeksi. Kuulostanee hurjalta, mutta kyseinen luonnehdinta ei varmasti ole hirveän kaukana todellisuudesta sillä sosiaalinen media pitää sisällään niin valtavasti ihmisten henkilökohtaisia tietoja. (Järvinen 2012, 294 – 295.) Ihmisten sosiaalisen median toiminta toimii materiaalina seuraamiselle, tilastoinnille ja analysoinnille. Blogimerkinnät, twiitit ja nettikeskustelut ovat pullollaan dataa, jonka perusteella voidaan päätellä tulevia trendejä ja vallitsevia mielipiteitä. Facebook itse on muun muassa kykeneväinen päättelemään käyttäjien toiminnan perusteella mahdollisen parisuhteen syntymisen henkilöiden välille. Tämä on tietenkin harmiton esimerkki siitä, mitä käyttäjistä kerätyllä tiedolla voidaan ennustaa. (Järvinen 2014, 275 – 276.) Käyttäjien on kuitenkin hankala täysin tietää mihin heidän tietojaan käytetään. Useimmat sosiaalisen median palvelut toimivat yhdysvaltalaisen lainsäädännön mukaan ja voivat täten hyödyntää käyttäjiensä henkilökohtaisia tietoja oman mielensä mukaan. Palveluun talletetusta tiedosta on täten tullut kauppatavaraa, jota myydään mainostajille ja muille kiinnostuneille tahoille. (Järvinen 2012, 294.) Usein käyttäjät suhtautuvat sosiaalisen median yksityisyyden ongelmiin toteamalla, ettei heillä ole mitään salattavaa. Todellisuudessa kaikki omaavat salaisuuksia, eikä kukaan oikeasti halua koko elämänsä kirjon olevan netissä luettavana. Verkkoon toimitetut tiedot saattavat johtaa myöhemmässä elämässä kiusallisiin tilanteisiin. Käyttäjien seuranta ja sosiaalisen median myötä syntynyt verkossa jakamisen kulttuuri on johtanut tilanteeseen, jossa yksityisyydestään tarkka henkilö joutuu usein perustelemaan miksi haluaa pitää asiat yksityisenä. Lähtökohtaisesti ainakin ennen henkilö on saanut pitää kaiken muun yksityisenä, jos niin haluaa, ja paljastaa vain haluamansa tiedot. (Järvinen 2014, 179.) Kyse on myös periaatteesta: mikäli kukaan ei ole kiinnostunut tietojensa suojelemisesta, palvelut ja tahot muuttuvat vain enemmän häikäilemättömiksi. Vaikka ei vielä olisikaan kovin huolestunut siitä mihin omat tiedot joutuvat, valveutunut sosiaalisen median käyttäjä kuitenkin pitää silmät auki ja tiedostaa palveluihin liittyvät mahdolliset riskit.

Tärkeä osa turvallista sosiaalisen median käyttöä on omiin yksityisasetuksiin tutustuminen. Oletusarvoisesti sosiaalisessa mediassa miltei kaikki tieto on julkista. Palveluntarjoajan tavoitteena on haalia mahdollisimman paljon käyttäjiä, kerätä mahdollisimman paljon julkista tietoa heistä ja levittää sisältöä mahdollisimman laajalle. Käyttäjien tietosuojan kannalta hillitympi tietojen leviäminen ja julkisuus olisi parempi. Oikein asetetut tietoturvaa ja tietojen jakamista

koskevat yksityisyysasetukset estävät ventovieraita näkemästä käyttäjän kaikkia henkilökohtaisia tietoja, kirjoituksia ja muuta sisältöä. Tietoturvallisempi valinta on sallia vain esimerkiksi omiin kontakteihin rajatulle ryhmälle pääsy näihin tietoihin. Tästä on tietenkin eniten hyötyä, mikäli on käyttänyt jonkinlaista harkintaa suodattaessaan kenet hyväksyy kaveriverkostoonsa sosiaalisessa mediassa. Kaikkia ei ole pakko hyväksyä kaveriksi sosiaalisessa mediassakaan ja tuhansista etäisesti tutuista tai jopa tuntemattomista koostuva kontaktiverkosto voi jopa osoittautua tietoturvariskiksi. Paras on hyväksyä verkostoonsa vain kontakteja joihin luottaa ja joiden oikeellisuudesta on varma. (Rousku 2014, 206 – 207.)

Internetiin kirjoittaessa on syytä ymmärtää, että nettiin kirjoitettu tai muuten toimitettu materiaali tulee siellä todennäköisesti pysymään jossain muodossa ikuisesti. Julkisissa sosiaalisen median palveluissa ei voi ikinä olla täysin varma siitä, että omassa profiilissa julkaistu tieto tulee pelkästään pysymään omalla seinällä omien kavereiden nähtävänä. Täten on parasta käyttää harkintaa ja miettiä mitä netissä julkaisee tai kirjoittaa. Huomionarvoista on myös pohtia millaisen kokonaiskuvan antaa itsestään. Yksittäinen viesti ei välttämättä sisällä hirveästi erityisen mielenkiintoista sisältöä ja saattaa tuntua harmittomalta, mutta ajan myötä yksittäisten viestien ja muiden julkaisujen määrä muodostuu laajemmaksi kokonaisuudeksi. Millaisen kuvan näistä ulkopuolinen käyttäjä voi saada? Mitä jos työhaastattelija tutkisi profiilin antia? Verkkoon toimitettu sisältö voi tulla myöhemmin vastaan yllättävissä tilanteissa.

Hyvä käytäntö on julkaista sosiaalisessa mediassa vain tietoa jonka luokittelisi julkiseksi tiedoksi. Vaikka uskoisi viestien pysyvän oman pienen some-piirin sisällä, voi tieto kuitenkin livahtaa oman kaveripiirin ulkopuolelle yllättäviä reittejä pitkin. Kenties esimerkiksi kaverit eivät ole yhtä vastuullisia omien yksityisasetuksiensa kanssa ja keskustelut leviävät sitä kautta kaikkien nähtäville. Useilla organisaatiolla, esimerkiksi armeijalla ja työpaikoilla, on käytössä sosiaalisen median ohjeet jotka linjaavat työntekijöille käytäntöjä verkossa toimimiseen. Sosiaalinen media sisältää monia sudenkuoppia jotka organisaatiot mieluusti haluaisivat välttää. Työntekijöiden henkilökohtaisena kirjoitetut mielipiteet saatetaan herkästi tulkita organisaation virallisina kannanottoina ja sotilaiden tilapäivityksistä saattaa tulla ilmi arkaluontoisia tietoja esimerkiksi sotilasjoukkojen sijainnista. Tämän vuoksi organisaatiot ovat joutuneet asettamaan tiukkojakin vaatimuksia jäsentensä toiminnalle verkossa. Mikäli haluaa pysyä pomon hyvissä kirjoissa ja pitää työpaikkansa, olisi suotavaa noudattaa näitä linjauksia. Loppujen lopuksi kyseiset säännöt ovat usein hyvin järkeviä ja kohtuullisia ja ne myös suojelevat käyttäjiä itseään. Kiivaat poliittiset kannanotot kyseenalaisten aatteiden puolesta iltapäivälehtien kommenttipalstalla eivät muutenkaan ole sellaista sisältöä, jota nettiin kannattaa toimittaa. (Rousku 2014, 206 – 207.)

Joissain sosiaalisen median palveluissa voi tavanomaisen viestinnän ohella käyttää erinäisiä sovelluksia. Facebookissa esimerkiksi on tarjolla yli 10 miljoonaa erilaista sovellusta. Määrä on hurja ja mukaan mahtuu taatusti myös vaarallisia ja haitallisia sovelluksia, sillä sovellukset ovat ulkopuolisten tahojen

käsialaa. Tärkeää on varmistua sovelluksien turvallisuudesta ennen uuden sovelluksen hyväksymistä. Hyvä käytäntö on esimerkiksi jollain internetin tiedonhakukoneella tutkia, mitä verkossa kyseisestä ohjelmasta sanotaan, jos sovellus vaikuttaa hieman epäilyttävältä. (Rousku 2014, 207.)

Sosiaalisen median vaikutus ulottuu palvelun ulkopuolisillekin sivuille. Iltapäivälehtien artikkeleita voi kommentoida usein Facebook-tiliä käyttämällä ja kaikenlaisista asioista netin syövereissä voi tykätä, vaikka ei edes oltaisi Facebookissakaan. Käyttäjän selailusta saatetaan myös kerätä tietoja evästeiden avulla. Mikäli ei halua sosiaalisen median palveluiden seuraavan palvelun ulkopuolista selailua, on järkevää muistaa kirjautua ulos kun ei enää käytä palvelua. (Järvinen 2012, 309.)

8 YHTEENVETO

Tietoturvasta on muodostunut todellisesti merkittävä ja tärkeä osa arkipäiväisen elämän toimimista. Tietoturvan pettäessä arkipäiväiset askareet ja työtehtävät saattavat hetkessä muodostua haasteellisiksi tai jopa mahdottomiksi suorittaa. Jokainen tietoyhteiskunnan jäsen törmää tietoturvaan niin töissä ja arkisessa aherruksessa, kuin myös lomaillessa kaukana tavanomaisista päivittäisistä haasteista. Palvelut, työtehtävät, henkilökohtaiset tiedot ja kavereiden kanssa vapaa-ajan vietto yhdistyvät kaikki internetin valtavassa maailmassa. Jokaisen käyttäjän vastuulla on varmistua omasta turvallisesta toiminnasta netissä.

Merkittävä osa kaikenlaista verkossa toimimista on tunnistautuminen internetissä sijaitsevien palveluiden käyttäjäksi. Tämä tapahtuu usein käyttäjänimen ja salasanan avulla. Käyttäjänimen ollessa useimmiten yleistä tietoa, korostuu salasanan merkitys käyttäjän tunnistamisessa. Yhden tunnuslauseen tai -sanan tietäminen erottaa oikean käyttäjän väärästä. Tämän vuoksi hyvän ja vahvan salasanan valitseminen on tärkeää. Merkkien määrän kasvaminen vahvistaa salasanaa merkittävästi ja tekee sen selvittämisestä vaikeampaa rikollisille. Pitkän salasanan voi muodostaa esimerkiksi käyttämällä salasanalausetta tavanomaisen yhden sanan tunnussanan sijaan. Yleisin haaste salasanojen saralla on niiden muistaminen. Salasanakäytännöt ovat muotoutuneet niin monimutkaisiksi, jotta salasanoista on tullut usein ihmisille vaikeita muistaa mutta samalla koneille helppoja laskea ja selvittää. Kokonainen lause salasanana tai kenties lauseen ensimmäisistä kirjaimista muodostettu yhdistelmä saattaa olla epämääräisten kirjaimien ja merkkien sekasotkua helpompi muistaa. Teoriassa salasanoja ohjeistetaan vaihtamaan ahkerasti. Käytäntö kuitenkin osoittaa, että käyttäjät vaihtavat salasanoja melko laiskasti. Kultainen keskitie ja hyvä kompromissi käyttömukavuuden ja tietoturvan välillä olisi vaihtaa tärkeiden palveluiden salasanoja kohtuullisen ajan välein. Salasanaa valitessa kannattaa välttää yleisesti käytettyjä huonoja salasanoja. Mahdollinen tunkeutuja kokeilee todennäköisesti ensimmäiseksi kaikkia maailman yleisimpiä salasanoja. Myös yleisiä helposti esimerkiksi sosiaalisesta mediasta selvitettäviä tietoja kannattaa välttää kaikissa tunnistautumiseen liittyvissä kohteissa. Salasanaksi on huono idea valita suosikkiurheilujoukkueen nimeä ja tietoturvakysymyksen vastaukseksi ei kannata valita vastausta jonka kaikki muutkin tietävät, sillä näiden tarkoitus on varmistaa että juuri sinä käytät omaa tiliäsi.

Tietokoneella turvallisen työskentelyn takaamiseksi olisi tärkeä oppia tunnistamaan, että kaikki toimii niin kuin pitääkin. Tietenkin tätäkin tärkeämpää on huomata jos jokin on pielessä eikä toimi niin kuin pitäisi. Olennainen osa turvallista netissä asiointia on opiskella, miten oma selain kertoo käyttäjälle salauksien ja varmenteiden käytöstä. Joissain selaimissa tämä näkyy vihreänä lukkona, toisissa lukkona selaimen alaosassa ja joissain HTTPS tekstinä osoiterivillä. Salauksen ja sivuston varmennuksen toimiminen on joka tapauksessa tärkein osa turvallista yksityisten tietojen siirtämistä netin välityksellä. Huomionarvoista on myös huolehtia siitä, että internetissä asiointiin käytetystä verk-

koselaimesta on käytössä tuorein versio. Tämä takaa osaltaan selaimen turvallisuuden sillä mahdolliset tiedossa olevat tietoturva-aukot ovat täten selaimesta tilkitty.

Päivitykset ovat korjauksia ja parannuksia ohjelmien toimintaan ja tietoturvaan. Ohjelmien ja eritoten käyttöjärjestelmän päivittäminen on täten tietoturvankin kannalta tärkeää.

Virustorjunta ja toimiva palomuuri tekevät olennaista työtä tietokoneen suojelemiseksi. Virustorjunta etsii, tuhoaa ja estää haitallisia ohjelmia. Palomuuri taasen suodattaa tietokoneen ja internetin välistä liikennettä, pyrkien hyväksymään tarpeellisen liikenteen sekä pysäyttämään kaiken tietoturvaa uhkaavan liikenteen. Palomuurin tehtävä on suojata käyttäjää ulkopuolisilta uhilta. Palomuurin puuttumista ei voi paikata ja se tekee korvaamatonta työtä suojellessaan laitteita haitalliselta verkkoliikenteeltä.

Haittaohjelmia on hyvin monenlaisia, mutta yleispätevästi kaikkia niitä voisi luonnehtia ohjelmiksi, jotka ovat aiheuttavat koneelle päästessään käyttäjälle harmia tai jopa suoranaista haittaa. Ohjelmien kirjo on laaja ja ne voivat levitä monin eri tavoin. Haittaohjelma saattaa päästä livahtamaan koneelle sähköpostin liitetiedostona, levitä saastuneesta tallennuslaitteesta, tarttua haitalliselta www-sivulta, hyödyntää tunnettua tietoturva-aukkoa ohjelmassa tai yllättää kaverin toimittaman linkin takaa sosiaalisessa mediassa. Mahdollisuuksia on monia ja siksi paras tapa varautua on minimoida riskien määrä: päivittää verkkoselain, käyttöjärjestelmä ja muut ohjelmat, käyttää virustorjuntaa ja palomuuria sekä olla itse valpas ja vastuuntuntoinen verkon käyttäjä. Epäilyttävillä sivuilla ei kannata vierailla ja oudolta vaikuttavia linkkejä tai liitetiedostoja ei kannata avata. Haittaohjelmista on muodostunut osa rikollisten tahojen toimintaa ja näin ollen itse ohjelmatkin ovat muuttuneet ammattimaisemmiksi ja ilkeämmiksi. Usein tällaiset ohjelmat saattavat jopa pyrkiä aiheuttamaan uhrilleen taloudellista tappiota kiristämällä käyttäjää tai ryöväämällä rahaa pankkitililtä. Haittaohjelmien ollessa näin hurjia on syytä varautua etukäteen ja turvata laitteet niin hyvin kuin suinkin mahdollista.

Toinen yleinen tapa jolla rikolliset yrittävät aiheuttaa uhreille vahinkoa verkossa on tietojenkalastelu. Kyseessä on henkilökohtaisten tietojen utelua, usein jonkinlaisen huijauksen varjolla. Rikollinen huijaa käyttäjän luovuttamaan vapaaehtoisesti yksityisiä tietojaan, esimerkiksi pankkitietoja. Usein kyseessä voi olla vaikkapa kovin aidon oloinen yhteydenotto sähköpostitse pankin toimesta, jossa pyydetään syystä tai toisesta kirjautumaan sähköpostilinkin takana sijaitsevaan palveluun ja syöttämään sitten kosolti henkilökohtaisia tietoja. Nyrkkisääntö kuitenkin on, että suomalaiset pankit eivät koskaan ota asiakkaisiinsa yhteyttä sähköpostitse. Kaikkiin palveluihin kannattaa myös varatoimenpiteenä aina siirtyä kirjanmerkin kautta tai kirjoittamalla osoite omin käsin osoiteriville. Sähköpostilinkkien availu on riskialtista.

Tietokoneelle säilöttyjen tiedostojen ja tietojen hallinta mielletään yleensä tärkeäksi osaksi tietoturvaa. Tiedostojen turvallinen säilytys on tärkeää, mutta tärkeiden tiedostojen oikeaoppinen tuhoaminen on myös olennainen osa tietojen turvallista hallintaa. Tietojen säilyttämisen suhteen on tärkeä muistaa, että kiintolevyt ja USB-muistit ovat väliaikaisia tiedon tallennuslaitteita, sillä kaikkien näiden laitteiden suunniteltu toiminta-aika on rajallinen. Tallennusvälineitä kuten esimerkiksi kiintolevyjä, DVD- tai CD-levyjä, USB-muisteja yms. ei ole suunniteltu kestämään ikuisesti. Ne tulevat hajoamaan jossain vaiheessa. Tärkeiden tiedostojen varmuuskopiointi muihinkin palveluihin ja laitteisiin on täten erityisen tärkeää. Viisasta on myös pyrkiä sijoittamaan varmuuskopioidut tärkeät tiedostot talteen jonnekin muualle kuin alkuperäisen tallennuslaitteen välittömään läheisyyteen. Näin tulipalon, luonnonkatastrofin tai konevarkauden sattuessa varmuuskopio ei häviä alkuperäisen laitteen mukana, vaan on löydettävissä esimerkiksi toimistolta tai netin pilvipalvelusta. Tärkeiden ja arkaluontoisten tiedostojen tuhoaminen on suotavaa suorittaa asianmukaisella tavalla, kun niitä ei enää tarvitse. Pelkkä levyn alustaminen ei riitä puhdistamaan tallennuslaitetta tiedoista, sillä alustus ainoastaan poistaa tiedoston sijainnista levyllä kertovan kirjanpidon. Mikäli haluaa olla varma tietojen häviämisestä, kannattaa levyltä poistaa tiedot asianmukaisella apuohjelmalla tai tuhota koko fyysinen levy esimerkiksi vasaralla hakaten.

Uusin käänne ihmisten yksityisyyden suojelemisen ja tietoturvan saralla on vallitseva innostus dokumentoida kaikki tiedot, ihmissuhteet ja elämäntapahtumat verkkoon sosiaalisessa mediassa. Sosiaalisesta mediastahan tekee juuri kiinnostavan tietojen ja sisällön jakaminen, mutta toisaalta samalla se asettaa yksilöiden tietosuojan varsin pulmalliseen tilanteeseen. Verkossa on tätä nykyä niin kosolti tietoja aktiivisesta sosiaalisen median käyttäjästä, että yksityisyyttä ei enää juuri ole olemassakaan. Julkaistessa tietoja internetissä tulisi kuitenkin ymmärtää, että tiedot todennäköisesti joutuvat myös oman tuttavapiirin ulkopuolisten tahojen nähtäväksi. Täten kannattaa pohtia tarkasti, minkälaista tietoa julkaisee netissä. Esimerkiksi lomamatkasta kertominen saattaa tuntua harmittomalta, mutta tarkemmin ajateltuna haluaisitko sittenkään ilmoittaa kaikille avoinna olevassa blogissa talon olevan tyhjillään parisen viikkoa? Tärkeää on ymmärtää, että pahimmassa tapauksessa kaikki mitä nettiin toimittaa myös jää sinne. Vähemmän imartelevat kuvat kosteilta syntymäpäiväjuhlilta tai epäasialliset poliittiset kannanotot saattavat hetkessä tallentua netin syövereihin, vaikka tiedon alkuperäinen toimittaja tulisikin myöhemmin katumapäälle ja poistaisi viestin. Tämän vuoksi aina kannattaa harkita tarkasti sisällön asiallisuutta ennen kuin päättää julkaisusta. Epäasiallinen tai muuten vain kiusallinen sisältö saattaa tulla myöhemmin vastaan yllättävissä asiayhteyksissä.

Tietokoneiden ja muiden älylaitteiden perimmäinen tarkoitus on helpottaa ihmisten elämää ja avata uusia ennennäkemättömiä mahdollisuuksia. Tietotekniikka tuo palvelut ja viihteen käyttäjien olohuoneisiin, yhdistää yhteisöjä ja ystäviä sekä tarjoaa ennennäkemättömän määrän tietoa johon kaikilla on mahdollisuus tutustua halutessaan. Turvallisesti ja oikein käytettynä tietotekniset laitteet rikastavat käyttäjiensä elämää ja tekevät ennen kaikkea elämästä helpompaa.

LÄHTEET

Andreasson, Ari & Koivisto, Juha 2013: Tietoturvaa toteuttamassa
Tietosanoma, Helsinki

Hakala, Mika 2006: Tietoturvallisuuden käsikirja
Docendo, Jyväskylä

Järvinen, Petteri 2006: Paranna tietoturvaasi
Docendo, Jyväskylä

Järvinen, Petteri 2012: Arjen tietoturva: vinkit & ratkaisut
Docendo, Jyväskylä

Järvinen, Petteri 2014: NSA: näin meitä seurataan
Docendo, Jyväskylä

Poliisi, CERT-FI ja F-Secure Oyj: Ransomware
http://www.ransomware.fi
Viitattu: 15.2.2016

Rousku, Kimmo 2014: Kyberturvaopas: tietoturvaa kotona ja työpaikalla
Talentum, Helsinki

Suomen Internetopas: Tietokonevirukset
http://www.internetopas.com/yleistietoa/virukset/
Viitattu: 7.2.2016

Viestintävirasto: Langattomien verkkojen suojauksessa käytetty WPS-tekniikka murtuu helposti
https://www.viestintavirasto.fi/kyberturvallisuus/tietoturva-nyt/2012/01/ttn201201041606.html
Viitattu: 2.4.2016

Viestintävirasto: Suojaamattoman WLAN:n käyttö
https://www.viestintavirasto.fi/kyberturvallisuus/tietoturva-nyt/2014/09/ttn201409171602.html
Viitattu: 24.2.2016

Viestintävirasto: Haittaohjelma saattaa varastaa tietoja tai louhia virtuaalivaluuttaa
https://www.viestintavirasto.fi/kyberturvallisuus/tietoturva-nyt/2015/02/ttn201502181338.html
Viitattu: 7.2.2016